SafeNet ProtectDrive™

Administration Guide

© 2012 SafeNet, Inc. All rights reserved.

Part Number 007-011122-001 (Rev E, August 2012)

Software Version 9.4.2

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support. SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608
Email: support@safenet-inc.com

Acknowledgements

- ProtectDrive includes software developed by Apache Software Foundation (http://www.apache.org/).
- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
- Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
- Windows 7 is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Relevant Documentation

Basic configuration procedures for token support are discussed in this manual. For detailed installation and configuration information relevant to SafeNet's Borderless Security tokens, please refer to the following documents:

- *Borderless Security PK and SSO Administration Guide*
- *Borderless Security PK and SSO User Guide*
- *iKey 1000 Series Developer's Guide*

Table of Contents

Chapter 1 Introduction 1
Product Overview 1
ProtectDrive Variants 2
Who Should Read This Document? 2
Chapter 2 ProtectDrive Functional Description 3
Supported Pre-boot User Authentication Credentials 3
Misplaced/Forgotten User Authentication Credentials 4
Unattended Reboot Followed by Automatic Pre-boot Authentication 4
Windows User Authentication 5
Single Sign-on (SSO) 5
Manual Windows Authentication 5
Borderless Security (BSEC) Authentication 5
Single Sign-on in a Non-Windows Environment 5
ProtectDrive Notification Icon 6
Hard Drive and Removable Media Encryption and Decryption 7
ProtectDrive System and User Policy 7
Remote Management 7
Local Management 8
Central Management via Active Directory or ADAM 8
ProtectDrive Central Management Using ADAM 9
Windows Domain Preparation for Central Management 9
ProtectDrive Recovery Files and Key Management 10
ProtectDrive Disaster Recovery 11
ProtectDrive Licensing 11
License.txt Installation 12
Authorization.txt Installation 12
What Happens if Internet Access is Unavailable? 12
Chapter 3 System Requirements 15
Minimum Hardware Requirements 15
Supported Storage Hardware 16
Device Access Control 16
Supported Operating Systems 17
For Client Management (on Server) 17
For Client 17
Supported Networks 18

Chapter 4 ProtectDrive Software Compatibility 19
DOS Drivers and TSRs 19
Other Disk Encryption Products and Security Components 19
iolo System Mechanic Professional® 19
Windows and Third-party Boot Managers 19
Windows BitLocker® and BitLocker To Go™ Drive Encryption Utilities 19
Windows Disk Manager Utility 20
Windows Fast User Switching Utility 20
Windows Folder Compression Utility 20
Windows System Restore Utility 20

Chapter 5 Deploying ProtectDrive 21
Best Practices 21
Fingerprint Authentication 21
Storage System Preparation 21
Back Up the License File 22
Recovery File Set Preparation 22
Sector 0 Backup (for Removable Media only) - Optional 23
Custom Recovery Key Set Creation 24
Certificate Wizard Procedures 25
Remove ADAM Instance and Unused ADAM SCPs 32
Configure the Windows Firewall for ADAM 35
Enable ADAM or AD LDS on a Member Server 36
ProtectDrive Install (MSI) Package 41
Customizing the MSI Package 41
ProtectDrive MSI Properties 42
Deploying Administrative Management Tools 45
How has the ProtectDrive Installation Changed? 45
Prepare the Windows Domain 45
Install the ProtectDrive Administrative Management Tools 51
What are the ProtectDrive Administrative Management Tools? 55
ProtectDrive Management Console 55
Deploying Client-Side Components 64
Custom Graphics File 64
Install the ProtectDrive Client-Side Components 64
Customizing the Installation 71
Disk Imaging—Norton™ Ghost™ Interoperability with ProtectDrive (version 9.0 and higher) ... 79
Using Norton Ghost™ in RAW Mode 79
Creating a Unique Disk Key for Each Deployed System 80
Upgrading From a Previous Version of ProtectDrive 81
Before You Begin 81
Creating a New Recovery File Set 82
About Interactive Upgrades 82
About Silent/GPO Upgrades 82
Upgrade Procedure 83

 © SafeNet, Inc.

Uninstalling ProtectDrive 84
Windows Vista *84*
Windows 2003, 2008, or XP *85*
Windows 7 ..... *85*
Removable Media Recovery 86
Standard Recovery Procedure *86*
Alternate Recovery Procedure #1 (Use RmRMBR) *87*
Alternate Recovery Procedure #2 (Use Sector 0 Backup Data) *88*
Exporting the Client Configuration Settings (.XML file) 89
Importing the Client Configuration Settings (.XML file) 91

Chapter 6 Single Sign-On Management 94
Introduction 94
Accessing the Single Sign-On Assistant *94*
Windows Authentication *95*
Post-Authentication Accounts *95*
RSA SOM Support 96
Overview *96*
Implementation *96*
Considerations *96*
Third-Party Product Support 97
Overview *97*
Support for Third-Party GINAs *97*
Support for Third-Party Accounts *97*
Administrative Procedures 98
Configuring After ProtectDrive Installation Over an Existing System *98*
Configuring After Installing Additional Software to the ProtectDrive System *98*
Changing Chained GINA *99*
Setting GINA Configuration *99*
Creating a Post-Authentication Account *100*
Modifying a Post-Authentication Account *102*
Removing a Post-Authentication Account *102*
Creating a Post-Authentication Account Field *103*
Modifying a Post-Authentication Account Field *104*
Removing a Post-Authentication Account Field *105*
Exporting SSO Settings *105*

Chapter 7 Configuring Default System and User Policy 106
Configure Default Settings in Active Directory Users and Computers (ADUC) MMC Snap-in 106
Configure Default Settings in ProtectDrive Management Snap-in 108
PD Settings Tab – Configure the Default System Policy 109
Authentication Settings *109*
Advanced Settings – Accessibility Options *114*
Advanced Settings - Allowed Certificate Usages *116*
Advanced Settings - Default Permissions (Device Access) *118*
Advanced Settings - Encryption *119*
Advanced Settings - Interrupt Vector Update *121*

Advanced Settings - Lockout *122*
Advanced Settings - Management *123*
Advanced Settings - Password Policy *124*
Advanced Settings - User Interface *126*
Status Settings *127*
PD Users Tab – Configure the Default User Policy 129
License Manager Tab – View/Install/Update License 133
Upgrade to a Full License From License Manager *134*
Upgrade to a Full License From the Nag Screen *134*

Chapter 8 System and User Management 136

Manage System Policy From the Server 136
Manage User Policy From the Server 141
Assigning Users to Clients and Managing User Policy via the Computer Object *141*
Managing User Policy via the User Object or Group Object *142*
Manage System and User Policy Locally 144
PD Settings Tabs *144*
PD Users Tab *145*
Change a Pre-boot Password 146

Chapter 9 User Authentication 147

Authenticate with Smart Card/Token and PIN/Fingerprint 148
Pre-boot Authentication *148*
Windows Authentication *149*
Token Removal Policy *150*
Authenticate with Username, Password, and Domain Name 151
Pre-boot Authentication *151*
Windows Authentication *152*
Helpful Hints 153

Chapter 10 Extraordinary Authentication Scenarios 155

Emergency Logon for Token Users Procedure 156
End-User Instruction *156*
System Administrator Instruction *157*
Emergency Logon With Username Procedure 159
End-User Instruction *159*
System Administrator Instruction *160*
Emergency Logon Without Username Procedure 162
End-User Instruction *162*
System Administrator Instruction *163*
Unattended Reboot and Automatic Pre-boot (APB) Authentication 164
Creating a Disaster Recovery Disk Key 166
Create the Recovery Disk Key *166*
Recover (Decrypt) the Disk *168*

 © SafeNet, Inc.

Chapter 11 RapidRecovery™ Disaster Recovery Tools 169
Introduction 169
BACKUP.EXE – Creating ProtectDrive Recovery Files 169
DECDISK.EXE - Disk Decryption Utility 170
Using Recovery Files 172
Manually Specifying the Decryption Area 172
DISPEFS.EXE – ProtectDrive Diagnostic Utility 173
PDUSERDB.EXE – Pre-boot User Database Administration Utility 174
PEPREP.EXE – WinPE Bootable Recovery Disk Utility 175
Sample Scenario 175
Create the WinPE Bootable Recovery Disk 175
Inject the ProtectDrive Disk Key 176
Map a Network Drive 177
PEPREP Command Line Options 177
RMBR.EXE – MBR Recovery Utility 178
RMBR Initial Status Check 178
RMBR Version Compatibility Check 179
Restoring the ProtectDrive MBR (RMBR /p) 179
Restoring the Original MBR (RMBR /o) 180

Chapter 12 Troubleshooting and Reporting Information 181
Switch from the Default to Legacy Pre-boot (Temporary) 181
Switch from the Default to Legacy Pre-boot (Permanent) 181
Disk Encryption Warning 181
ProtectDrive User Authentication Activity Tracking 182
Incorrect Pre-boot Username and/or Password 182
Pre-boot Log On Failure Due to System Inoperability 182
Disallowed Device Access Errors 183
Disallowed Local Windows Authentication Error 183
Disallowed Post-boot Windows Domain Authentication Error 183
Event Viewer Log 184
Active Directory/ADAM Reporting Script 185
ProtectDrive Server with Active Directory 185
ProtectDrive Server with ADAM 186
Sample Report Output 186

Appendix A Smart Card/Token & PIN User Authentication 187

Appendix B Username/Password/Domain Authentication 189

Appendix C Post-boot User Authentication into Windows 191

Appendix D System Debug and ACS Error Messages 193
System Debug 193
ACS Error Messages 196

Appendix E Additional Guidance Regarding Security 203
Evaluated Versions of ProtectDrive 203
Guidance for Users of ProtectDrive 204
Further Reading Relevant to the CC Certification 204
Product Identification 204
Before Installation 204
After Installation 204
Organizational Requirements 205
Connections to Outside Systems 205
Guidance 205
Tampering 205
Training 205
Tokens 205
Users 205
Device Permissions 205
Guidance for the Operating System Configuration 206
General 206
Password Policy 206
Screen Lock Feature 206
Information Relevant to Administrators of ProtectDrive 207
Operating Systems 207
Evaluated Items 207
Encryption Algorithm 207
Display Warning When Disks Not Fully Encrypted 207
Automatic Pre-boot Authentication 207
Show Unsuccessful Logon Warnings 207
Access Control 207

Appendix F iKey Management 209
iKey 1000 209
Manage the iKey 1000 Through the iKey SDK 209
iKey 2032 211
SafeNet Token Manager Utility 211
Web Enrollment 213

Appendix G Supported Smart Cards, Tokens, and Readers 221
Smart Cards 221
Tokens 222
Smart Card Readers 223
Removable Devices 224

 © SafeNet, Inc.

Chapter 1
Introduction

Product Overview

In today's computing environment, hard disk drives (HDD) have become mass repositories of proprietary information. The widely used Windows operating systems provide adequate data privacy, whether on a stand-alone PC or a networked computer (in most operating environments). However, insufficient data security protection exists in a case of system (or HDD) loss due to malicious intent. Unless appropriate data protection measures are taken, any HDD can be removed from the system, and data on it may be read.

To bridge these data security gaps, SafeNet has developed the ProtectDrive (PD) system security and data encryption application. SafeNet ProtectDrive is a multi-user Windows Active Directory-aware computer security application. It provides the following functionality listed in order of appearance during normal ProtectDrive operation:

Pre-boot User Authentication (32-bit pre-boot is the default)	Used to derive unique decryption keys for decrypting the operating system files and the rest of the encrypted hard drive(s). Support for smart cards/tokens and PINs/fingerprint authentication, as well as Windows Domains, Usernames, and Passwords. Support for auditory prompting during pre-boot authentication for the visually impaired (for example, prompts occur for a number of screen states or conditions, such as smart card or token insertion, successful logon, and unsuccessful logon. For details, refer to page 114).
Emergency Pre-boot User and Token Logon Recovery	Smart card/token user logon recovery and Windows Domain user pre-boot logon procedures, which includes emergency one-time logon with or without a username at pre-boot.
Single Sign-on or Manual Windows Authentication	ProtectDrive provides Automatic Windows (Domain) user authentication following successful pre-boot authentication. Manual authentication is also available as an alternative. Single sign-on is currently not supported with fingerprint logon.
Configurable System and User Policy	Device access control of fixed disks and removable media. Policy management using the MMC snap-ins. Automatic System and User Policy data replication from the server.
Hard Drive and Removable Media Encryption	Strong data encryption made completely transparent to the user.
Disaster Recovery Tools	MS-DOS utilities used to recover corrupt and/or inoperable systems.

ProtectDrive Variants

ProtectDrive is available in two variants—*ProtectDrive* and *ProtectDrive for Servers*. Each variant has its own documentation suite.

- **ProtectDrive**—This standard edition is targeted for workstations and laptops.
- **ProtectDrive for Servers**—This edition is targeted for server operating systems. Servers have unique full disk encryption requirements compared to workstations and laptops. *ProtectDrive for Servers* operates seamlessly with hardware-based RAID systems, rendering removable disks unreadable to unauthorized parties outside of the original (or recovered) server system.

Who Should Read This Document?

This document is intended for System Administrators who are resposibile for configuration and maintenance of various computer system components such as ProtectDrive.

You must have administrative privileges to install and configure ProtectDrive. Use this document as a guide for ProtectDrive deployment on stand-alone and networked multi-user computer systems with single-boot configurations, for issues pertaining to ProtectDrive installation, data encryption, system and user management, and disaster recovery.

© SafeNet, Inc.

Chapter 2
ProtectDrive Functional Description

Supported Pre-boot User Authentication Credentials

In order to boot an encrypted operating system partition ProtectDrive must get access to the *decryption keys* prior to the operating system boot. These keys are used for decrypting the operating system files as well as the rest of the encrypted hard drive(s).

For this purpose, ProtectDrive introduces the *Pre-boot User Authentication*. 32-bit pre-boot environment is the default, but the 64-bit and legacy 16-bit environments are also supported.

The decryption key is encrypted by a unique data key derived from the user authentication credentials. After user authentication, the disk key can be decrypted and the operating system can be loaded. In support of this functionality, ProtectDrive maintains its own *Pre-boot User Database* (**pduserdb**).

To assist the visually impaired, auditory prompting can be configured for pre-boot authentication. These prompts will occur for a number of screen states or conditions, such as smart card or token insertion, successful logon, and unsuccessful logon. For details, refer to page 114.

The ProtectDrive Pre-boot User database has the following characteristics:

- Maximum Number of Users/Certificates — 2,000
- Username Length/Syntax — 1 to 20 characters
- Password Length/Syntax — Up to 127 **case-sensitive** characters (no minimum). (Windows maximum password length is also 127.)

Although the maximum number of users is 2,000, three of these slots are reserved for ProtectDrive use only. The remaining slots are dedicated to your user database. However, keep in mind that each user can potentially use *multiple* user slots—one for their password, one for their shared key, and one for every certificate.

(32-bit environment only) A blank screen saver will automatically take effect when a workstation is left unattended for at least 10 minutes.

If the 32-bit version is already installed and there is a need to revert to the legacy 16-bit version, press the [Shift] key while the PC is booting (on some machines, the [Shift] key should not be pressed too early in the boot process). The PC will start in 16-bit pre-boot one time only (until the next reboot occurs).

ProtectDrive is capable of pre-boot authenticating users on stand-alone (Local Windows only) and Windows Domains systems. In addition to local password or domain password logon, the following user authentication credentials are supported by ProtectDrive:

Smart Card/Token and PIN/Fingerprint	This method of user authentication requires a token or smart card, and used for Windows smart card/token logon in an Active Directory environment. If fingerprint authentication is used, then the smart card/token must be initialized (as PKI cards) with BSEC middleware version 7.1.1 (or higher) prior to installing ProtectDrive. If ProtectDrive was installed before BSEC middleware, please contact SafeNet Technical Support. For BSEC installation and configuration details, refer to the *Borderless Security PK and SSO Administration Guide*.
Shared Key Token (iKey 1000) and PIN	This method of user authentication requires the presence of a shared key (**iKey 1000** only) at pre-boot. After pre-boot authentication occurs, Windows authentication is required. Refer to page 209 for basic information on iKey 1000 management. For a list of supported tokens and smart cards, refer to the latest ProtectDrive customer release notes on the SafeNet Web site, in the *Customer Care Center (http://c3.safenet-inc.com/secure.asp*).

Misplaced/Forgotten User Authentication Credentials

ProtectDrive will accommodate users who have misplaced their authentication credentials. This refers to such instances where, for example, a user has misplaced their smart card/token or forgotten their Windows Domain Password.

ProtectDrive System Policy provides automated procedures for handling these pre-boot authentication scenarios.

Unattended Reboot Followed by Automatic Pre-boot Authentication

Various System Administration functions not related to ProtectDrive may at times require an unattended reboot followed by automatic pre-boot authentication. ProtectDrive provides this functionality with the use of a special User Account. System Registry amendments are required to implement this functionality.

© SafeNet, Inc.

Windows User Authentication

Single Sign-on (SSO)

ProtectDrive System Policy can be configured to *automatically* authenticate users to Windows. Users are automatically logged on to their respective Windows Domain or Local Windows accounts following their successful pre-boot authentication. This method of automatic Windows authentication is referred to as *single sign-on*.

Single sign-on is currently not supported with fingerprint logon.

Not all smart card and reader combinations support SSO.

Manual Windows Authentication

As an alternative to the single sign-on mode, ProtectDrive System Policy can be configured to provide standard Windows authentication screens, allowing the user to manually authenticate into their respective Windows (Domain) account.

Borderless Security (BSEC) Authentication

When fingerprint authentication is used, single sign-on is not supported. When a user logs in to ProtectDrive with a smart card/token and fingerprint, a *Token Login* (BSEC) authentication screen will display for the user to log in to Windows. After the user's credentials are verified, the Windows desktop displays.

The system can be configured to accept up to four fingerprints. The number of fingerprints that are ~~–e~~nrolled" will determine the appearance of the login screen that displays. Refer to the *SafeNet Borderless Security PK and SSO User Guide* for details on fingerprint enrollment.

Single Sign-on in a Non-Windows Environment

In a Windows only, single sign-on user authentication environment, ProtectDrive will operate seamlessly without any required setup.

Alternatively, the *Single Sign-On Assistant* application (located in the install folder, *C:\Program Files\SafeNet ProtectDrive*) can be used to manage the configuration of ProtectDrive for seamless operation in a single sign-on user authentication system environment, where systems other than Windows are involved.

Single sign-on is currently not supported with fingerprint logon.

Refer to Chapter 6 for details on *Single Sign-On Assistant*.

ProtectDrive Notification Icon

The Windows *notification area* is a portion of the taskbar that displays system and program notifications and status.

If ProtectDrive has been configured with the **Show SafeNet ProtectDrive System Tray Icon** option enabled (in **PD Settings > Advanced > User Interface**), a small ProtectDrive icon is placed in the Windows notification area of the taskbar, located in the lower-right corner of the Windows Desktop. The icon indicates that the PC is secured by ProtectDrive.

If the **Show SafeNet ProtectDrive System Tray Icon** option is not enabled, then the ProtectDrive notification icon will not display at all.

During ProtectDrive-related operations, the icon changes to . This icon notifies the user that an action is underway, which is especially helpful during potentially lengthy or system resource-hungry tasks. ProtectDrive-related operations include:

- Activating or deactivating pre-boot authentication
- Encrypting or decrypting fixed and removable drives
- Processing remote configuration updates

Hover the mouse pointer over the icon to display a tooltip of the task that is in progress. The following example shows the tooltip for the encryption process of drive C.

© SafeNet, Inc.

Hard Drive and Removable Media Encryption and Decryption

All data encryption is invisible (transparent) to the end user. ProtectDrive automatically encrypts and decrypts multiple HDD partitions and selected removable media. Any authenticated computer that shares the encryptor's system key (created at installation time) can decrypt the removable media, provided the correct encryption password is entered.

When encrypted data is being read, ProtectDrive decrypts it —on the fly"— it's ready for display to the user or for use by other applications and software processes. All data written back to the HDD or removable media is automatically re-encrypted. Consequently, normal system operation remains unaffected.

ProtectDrive System and User Policy

Remote Management

System policy can be managed *remotely* for ProtectDrive clients through the **ProtectDrive Management Console** snap-ins.

These snap-ins—**ProtectDrive Management**, **ProtectDrive Reports**, and **Active Directory Users and Computers**—are installed during the ProtectDrive **Administrative Management Tools Installation**. (**Note:** This installation option replaced the **Typical Server Installation** option in ProtectDrive version 8.2.1).

The **Administrative Management Tools Installation** allows the administrator the flexibility to install the necessary tools wherever remote client management will take place (this could be on a server or even a workstation).

ProtectDrive clients with *their own unique configuration objects*—clients managed by the property sheet of their own computer objects–are managed remotely through the **ADUC** MMC snap-in. The central management of a computer object by ProtectDrive allows for central changes to affect only a specific computer. This is no different than the way clients were managed prior to ProtectDrive version 8.3.

In version 8.3 (and higher), groups of ProtectDrive clients that use *the same configuration object* are managed remotely through the **ProtectDrive Management** snap-in. An unlimited number of custom configuration objects can be created for any number of client sets. New configuration objects can be created and added to the **ProtectDrive Management** snap-in. Clients can be added to and removed from configuration objects any time. Refer to page 55 for details.

In version 9.4 and higher, **ProtectDrive Reports** is available to provide views of various status reports, such as **Update Status**—shows which clients have up-to-date settings and the last time they were updated, and **Encryption Status**—shows which clients are not encrypted, which are, and with what. Refer to page 61 for more on ProtectDrive Reports.

Local Management

System policy can be managed *locally* using the ProtectDrive **Local Management Console** utility (LMC), which is deployed as part of the installation of the ProtectDrive Client-side components.

The LMC allows you to make local configuration changes after ProtectDrive is installed. Users are assigned to client systems and user device access control permissions are configured using the **PD Users** tab. User policy defines individual user access permissions to all devices.

Central Management via Active Directory or ADAM

Active Directory is a widely deployed management platform that most enterprises already use to manage users and computers. Active Directory Application Mode (ADAM) is a mode of Active Directory which is designed for organizations that require flexible support for directory-enabled applications

ADAM was first released in Windows Server 2003 R2. It has been updated with new and improved features for Windows Server 2008, and is now called AD Lightweight Directory System (AD LDS). Excluding the section on installing/enabling ADAM or AD LDS in Chapter 5, all other references to *ADAM* in this document implies both *ADAM* and *AD LDS*.

ProtectDrive clients can be centrally managed by either Active Directory or ADAM. They will function virtually the same with either one.

The primary difference between Active Directory and ADAM is the way in which schemas are applied:

- With *Active Directory*, all domain controllers use the same schema. Schema changes are forest-wide.
- With *ADAM*, there can be only one ADAM configuration set (consisting of a unique ProtectDrive ADAM instance and any number of replicated ProtectDrive ADAM instances) with their own schema, and they are completely independent from the Active Directory schema. After a unique ADAM instance is created, replica instances for it may also be created, each of which replicating one or more directory partitions from the unique instance.

  ADAM replications can be created as a backup precaution. In the event the primary ADAM server is inaccessible, the clients can continue to be updated via a replicated (secondary) ADAM instance until the primary ADAM server is available again.

© SafeNet, Inc.

If a more than one instance is created, the system will randomly select an instance to take over for the primary.

For details on creating a unique ADAM instance and ADAM replication, refer to the **Directory Preparation Utility** described on page 45.

ProtectDrive Central Management Using ADAM

When ProtectDrive is used in combination with ADAM, an ADAM instance with a ProtectDrive Partition (CD=PDPartition) will be installed on the member server through a task performed in the **Directory Preparation Utility** (PDDirPrep). Refer to the next section for more information on this utility).

To use ADAM with ProtectDrive, ADAM must be installed *before* you run PDDirPrep. Then, PDDirPrep can be run before or after performing the ProtectDrive **Administrative Management Tools Installation**. Refer to page 55 for details.

In the event that the currently active ADAM instance fails, (which may be identified by errors about service unavailability from PDMC), close and reopen PDMC so it can sync up with another ADAM instance.

Windows Domain Preparation for Central Management

The **Directory Preparation Utility** (PDDirPrep) is used to prepare a Windows domain to manage remote ProtectDrive clients. PDDirPrep can be installed wherever and whenever it is needed.

The **PDDirPrep** can:

- Create one unique ProtectDrive ADAM instance (as well as replicas of that instance, if desired) on each domain (instead of using Active Directory). A replica uses the configuration and schema partitions replicated from the unique ADAM instance.
- Extend the Active Directory (or ADAM instance) schema on the primary domain with the attributes that are required to manage the ProtectDrive client System and User policies.

  Only Active Directory schema changes are forest-wide.
- Prepare (configure) each domain for remote client management by creating a *Default Configuration Object*. By default, all new clients in the domain will automatically be linked to the Default Configuration Object in the ADUC snap-in in the **ProtectDrive Management Console**. You must be logged in as the domain's administrator to perform this task.

For details on the **Directory Preparation Utility**, refer to page 55.

ProtectDrive Recovery Files and Key Management

During a ProtectDrive installation, a recovery file set can be created. These files are required to perform disaster key recovery and emergency logon procedures.

Alternatively, these files can also be created prior to an installation by using the **Certificate Wizard** utility, located in the *\Tools* directory on the ProtectDrive distribution CD. A recovery file set consists of the following:

- **Master Security Certificate (MSC)**—The **PdMaster.cer** and **PdMaster.pfx** files make up a public/private key pair. **PdMaster.pfx** is used to extract Disk Key Recovery information using the Remote Recovery Console (**rpadmin**). The **PdMaster.pfx** file is intended to be private, and as such, it must be securely stored and only accessible to individuals who can perform disaster recovery. **PdMaster.cer** is the public key component of the Master Security Certificate (MSC), and is intended to be used on each installation.

- **Recovery Support Certificate (RSC)**—The **PdRecovery.cer** and **PdRecovery.pfx** make up a public/private key pair. **PdRecovery.pfx** is used for Emergency Logon in the Remote Recovery Console (**rpadmin**). The **PdRecovery.pfx** file is intended to be private, and as such, it must be securely stored and only accessible to individuals who can perform password recovery (for example, Help Desk/Support personnel). **PdRecovery.cer** is the public key component of the Recovery Support Certificate (RSC) and is intended to be used on each installation.

- **Salt**—The **salt.cid** file is used to permit the sharing of removable media between ProtectDrive PCs.

- **Recovery Envelope**—This **RecoveryEnvelope.env** file is created for every client PC, and is required for Emergency Logon using the **Remote Recovery Console** utility (**rpadmin**). The client name is included in the file name as follows: **<computer name>_RecoveryEnvelope.env**.

For details on the **Certificate Wizard** utility, refer to page 25.

For details on the **rpadmin** utility, refer to *Chapter 10*.

© SafeNet, Inc.

ProtectDrive Disaster Recovery

For stand-alone ProtectDrive installations, disaster recovery preparation begins with periodic ProtectDrive system data backups. The ProtectDrive **backup** utility creates recovery files, which can be used to later decrypt a failed system. These files must be stored off the client system. The backup file set that is created by the **backup** utility is used in conjunction with the Master Security Certificate (MSC) to perform Disk Key Recovery.

In ProtectDrive 8.3 (and higher), periodic backups are not necessary for remotely managed ProtectDrive clients, as backup recovery files can be obtained from Active Directory.

ProtectDrive also provides a set of command line recovery tools which can be used to perform disk recovery tasks such as data decryption and Pre-boot User database management. These RapidRecovery™ tools are included on the ProtectDrive distribution CD and generally used by System Administrators only. Refer to Chapter 11 for details.

ProtectDrive Licensing

ProtectDrive licensing includes license codes to activate disk encryption, removable media, and Active Directory/ADAM management. Typically, ProtectDrive is sold with this complete functionality.

To install a full version of ProtectDrive, a license code or authorization code is required. Otherwise, you can only install the 30-day *trial version* of ProtectDrive for evaluation purposes. When a ProtectDrive license is purchased, you will receive a license file or an authorization file (.txt format).

Prior to installing ProtectDrive, copy the appropriate .txt file to a location that you can browse to during the installation process, or, for silent/GPO installations, the license.txt or authorization.txt file (do **not** change the name of the file that you received) must be in the same directory as the **SafeNet ProtectDrive.msi** file.

If a license has expired, update the license through **License Manager** or the nag screen that displays periodically after the license expired. Refer to page 133 for more details.

Any time the license changes, it is good practice to run the **backup.exe** utility to ensure your recovery files are up-to-date. Refer to Chapter 11 for details on the backup utility.

License.txt Installation

During the ProtectDrive installation, browse to the .txt license file to install the license(s). Refer to page 64 for detailed step-by-step procedures for a ProtectDrive client installation.

For silent/GPO installations, the file, **license.txt**, must be included in the same directory as the **SafeNet ProtectDrive.msi** file.

For single installations, make sure the appropriate .txt file is in a location that you can browse to during the installation process.

Authorization.txt Installation

Most deployments require an **authorization.txt** file. Client PCs should have Internet access to complete this type of installation. The client's firewall must allow access to the Internet on **port 80** or port **5094**. If Internet access is not available, refer to the next section.

During the ProtectDrive installation, browse to the .txt authorization file. For silent/GPO installations, the **authorization.txt** file must be included in the same directory as the **SafeNet ProtectDrive.msi** file. The SafeNet server (or authorized reseller) will automatically be contacted via the Internet to complete this licensing process.

When the authorization code is transmitted to the server, a license is granted in kind to the client, and the client installation is allowed to continue. At the same time, the customer's license count is decremented by one on the license server.

If the client license count is *depleted*, the server will deny the client a license, and a message will display, notifying you that the installation cannot be completed. Please contact your sales agent if you require additional licenses.

Refer to page 64 for detailed step-by-step procedures for a ProtectDrive client installation.

What Happens if Internet Access is Unavailable?

If you are attempting to perform a multi-licensed installation and Internet access is unavailable, you can only install the 30-day trial version. After the trial version is installed, however, you can install a fully licensed version of ProtectDrive once you have obtained a license.

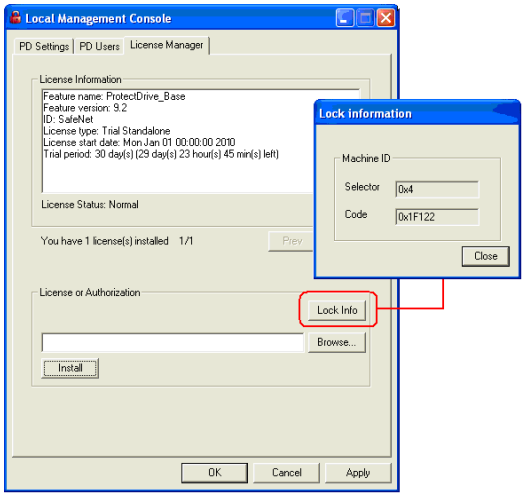
To obtain a locked license without an Internet connection, contact SafeNet Support (*support@safenet-inc.com or 800-545-6608*). A SafeNet Support representative will guide you through the following procedure to obtain the required information to issue you a license:

1. Open the **Local Management Console** on the client.

2. Click the **License Manager** tab.

© SafeNet, Inc.

3. Click **Lock Info**.



4. Read the **Lock Information** to the SafeNet Support representative.

5. The SafeNet Support representative will generate a license code and e-mail it to you in the form of a **license.txt** file. Use this file to complete the full license ProtectDrive client installation. Make sure you copy this file to a location that the client PC can browse to during the installation procedure.

   Any time the license changes, it is good practice to run the backup.exe utility to ensure your recovery files are up-to-date. Refer to Chapter 11 for details on the backup utility.

6. Upgrade to a full license. Refer to page 133 for detailed step-by step instructions to complete the license upgrade.

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Chapter 3
System Requirements

Minimum Hardware Requirements

- 32-bit Intel-compatible CPU computer system
- Sufficient memory to run the operating system, plus 150MB of free hard disk space
- CD ROM drive or access to a server based installation directory
- < 2TB HDD size limitation
- Client firewall must allow access to the Internet on **port 80**, or port **5094** if connection to the License Server is required.
- (Active Directory only) The Active Directory Server must have the following ports open to allow ProtectDrive clients to receive updates:
  - **port 88** TCP/UDP (Kerberos—network authentication protocol)
  - **port 135** TCP RPC (End Point Mapper; Distributed Component Object Model [DCOM] services)
  - **port 389** TCP/UDP (LDAP)
  - **port 1026** TCP (calendar access protocol; DCOM services)

  Ports **88** and **389** are required for proper communication of the domain member with the domain controller and Active Directory. Ports **135** and **1026** are specific to proper communication with the ProtectDrive server and its remote clients.

  Refer to page 35 for details on configuring the Windows firewall for ADAM.

Supported Storage Hardware

ProtectDrive can encrypt/decrypt all fixed (non-removable) system HDD partitions with a drive letter assigned (no hidden partition support), including all IDE/EIDE, SATA, SCSI drives, and selected removable media (such as USB external hard drives).

The *ProtectDrive* and *ProtectDrive for Servers* editions both support a hardware-based RAID system. Software RAID, however, is not supported.

ProtectDrive does not in any way interfere with the normal operation of the storage sub-system, with the following exceptions:

- It is not possible to format any partition on the system HDD.
- If a physical drive is partitioned into logical drives, it cannot be changed after ProtectDrive is installed.
- During installation, ProtectDrive accounts for all partitions present on the system. Post-installation partition resizing, converting, masking active, or re-partitioning is not supported. This includes the Master Boot Record manipulation.

Device Access Control

ProtectDrive System Policy and User Policy management consoles provide configurable default and individual user access rights to devices, such as removable media, diskettes, and CD-ROMs.

Floppy disk drives, removable devices such as CD-RW, DVD-RW, and Iomega Zip Drives are excluded from encryption and decryption. ProtectDrive does not interfere with the normal operation of these devices, but it does control configurable user read/write privileges to most of these devices.

© SafeNet, Inc.

Supported Operating Systems

This version of ProtectDrive is supported on the operating systems listed below.

For Client Management (on Server)

- Microsoft Windows Server 2003, Service Pack 2 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2, Service Pack 2 (32-bit and 64-bit)
- Windows Server 2008, Service Pack 2 (32-bit and 64-bit)
- Windows Server 2008 R2, Service Pack 1

For Client

- Microsoft Windows Server 2003, Service Pack 2 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2, Service Pack 2 (32-bit and 64-bit)
- Windows Server 2008, Service Pack 2 (32-bit and 64-bit)
- Windows Server 2008 R2, Service Pack 1
- Microsoft Windows XP Professional, Service Pack 2 or 3 (32-bit only)
- Microsoft Windows Vista, Service Pack 2 (32-bit and 64-bit)
- Microsoft Windows 7, all editions (32-bit and 64-bit)

Please note the following regarding Windows 7 Home editions:

- Only local passwords are allowed.
- Windows 7 Home computers cannot be members of a domain.
- ProtectDrive requires that Windows 7 Home accounts must be configured to require a login password.

The *ProtectDrive for Servers* variant cannot be installed on a non-server ProtectDrive system. The non-server edition of ProtectDrive will not allow client component installation on a Windows Server.

ProtectDrive supports the use of FAT16, FAT32, and NTFS file systems.

MS-DOS can be used during ProtectDrive Disaster Recovery. Inaccessible or corrupt ProtectDrive systems can be booted to MS-DOS from a floppy disk or CD. Drives that require special DOS drivers (for example, SCSI) or TSRs are only accessible to the ProtectDrive recovery tools, if the respective drivers are loaded.

Supported Networks

ProtectDrive is Active Directory-aware and fully supports Windows Domains. It does not interfere with normal operation of any of the Windows network services, including Remote Desktop connections. Windows Domain as well as Local Windows users are able to authenticate successfully into systems secured by ProtectDrive. All hard disk partitions encrypted with ProtectDrive are configurable as shared volumes at the discretion of the System Administrator.

© SafeNet, Inc.

Chapter 4
ProtectDrive Software Compatibility

ProtectDrive has been tested and does not interfere with normal operation of most MS Windows-compliant software, applications, services, and utilities. Some care needs to be taken, however, when using the following:

DOS Drivers and TSRs

When booted from a DOS floppy (or CD), ProtectDrive sees hard disks accessible via DOS drivers and TSRs if the appropriate drivers are loaded.

Other Disk Encryption Products and Security Components

ProtectDrive cannot be expected to function correctly if it is installed with another disk encryption product.

ProtectDrive is not compatible with Trusted Platform Module (TPM). If the machine is TPM-capable, then it must be disabled in the BIOS in order for ProtectDrive to operate properly.

iolo System Mechanic Professional®

It is not recommended that System Mechanic Professional® be installed on the same PC as ProtectDrive.

Windows and Third-party Boot Managers

At system start-up, ProtectDrive manipulates the Master Boot Record (MBR) while verifying its integrity. All software that needs to manipulate the MBR for its own purposes is **incompatible** with ProtectDrive. This also applies to the standard Windows boot manager.

Windows BitLocker® and BitLocker To Go™ Drive Encryption Utilities

It is not recommended that these utilities be used on a system that is encrypted with ProtectDrive.

Windows Disk Manager Utility

Any post-installation disk repartitioning, resizing, and mirroring configuration changes are prohibited by ProtectDrive. If any of the above operations are required, decrypt all disks and uninstall ProtectDrive before proceeding.

Windows Fast User Switching Utility

ProtectDrive disables the standard Windows **Welcome** screen along with its fast user switching functionality.

Windows Folder Compression Utility

Windows folder compression is fully supported, but with one exception: The ProtectDrive system files directory (*Securdsk)* must not be compressed on any partition.

Do not install ProtectDrive to a compressed system drive if the system drive is C: only. This will result in the compression of the *C:\Securdsk* directory, which will interfere with normal ProtectDrive operations.

Windows System Restore Utility

Windows System Restore points created prior to the ProtectDrive install are rendered useless. The system can only be restored to any restore point created following the ProtectDrive install.

© SafeNet, Inc.

Chapter 5
Deploying ProtectDrive

Best Practices

Review the sections below and make sure you have performed the appropriate procedures before and after installing ProtectDrive. You must have administrative privileges to install and configure ProtectDrive.

Before deploying ProtectDrive:

- Defragment the drives which will be encrypted by ProtectDrive.
- Repair any existing disk errors. The utilities provided by the hard disk manufacturer are typically the most robust tools for repairing disk errors.

Fingerprint Authentication

If fingerprint authentication will be used, before deploying ProtectDrive, the smart cards/tokens must be initialized (as PKI cards) with BSEC middleware version 7.1.1 (or higher) *prior to* installing ProtectDrive. If ProtectDrive was installed *before* the BSEC middleware, please contact SafeNet Technical Support.

For BSEC installation and configuration details, refer to the *Borderless Security PK and SSO Administration Guide*.

Storage System Preparation

Before deploying ProtectDrive:

- Ensure that your data storage system is well planned, and that no further rearranging of any of the partitions will occur. Use Windows Disk Management as needed to repartition, set up disk mirroring, resize partitions, etc.
- Run **CHKDSK /f** and the hard disk manufacturer's diagnostic utility to ensure file system health on all drives intended for encryption. Repair any bad sectors, should any exist, as ProtectDrive cannot encrypt them.
- Back up all important data prior to disk encryption.

Back Up the License File

Better safe than sorry. In the event that your hard drive requires reformatting or re-imaging after ProtectDrive has been installed, you'll need the existing ProtectDrive license file to re-install on the same machine.

If you do not have a backed up copy of the existing license file, you will be required to contact SafeNet for a new license file for the same machine, which could take longer to get the machine back up and running.

After ProtectDrive has been installed, follow these steps to preserve the ProtectDrive license file, and then store it in a safe location for future use, if it is ever necessary.

1. Go to *C:\Program Files\SafeNet ProtectDrive*.
2. Copy the **lservrc** file and save it to a safe location, preferably on another drive or computer (since you will be formatting this drive).
3. Rename the **lservrc** file to **license.txt**.
4. Use this **license.txt** file when you re-install ProtectDrive on the same machine.

Recovery File Set Preparation

SafeNet recommends that you create a Recovery File Set (saved on a floppy disk or CD, for example) that includes the ProtectDrive Recovery Tools and Recovery Keys. These files are required by the:

- ProtectDrive Disaster Recovery Tools
- Pre-boot Emergency Logon Procedures

After ProtectDrive has been installed on a system, follow these steps to create Recovery Disks.

1. Copy the **PdMaster.pfx**, **PdRecovery.pfx**, **salt.cid**, and **<computer name>_RecoveryEnvelope.env** files to a Recovery Disk CD. These files are created during the installation. (The PdMaster.pfx, PdRecovery.pfx, and salt.cid files can also be created pre-installation.)

2. Copy the contents of the *\Tools* directory (the ProtectDrive recovery tools) from the ProtectDrive distribution CD to the Recovery File Set location (a floppy disk or CD, for example).

3. On a separate CD, copy the EFS recovery files (produced by running *backup.exe*, or obtained from Active Directory). These files are required for disaster disk key recovery. Refer to page 168 for details about this recovery procedure.

© SafeNet, Inc.

Sector 0 Backup (for Removable Media only) - Optional

As an added level of assurance to recover a failed removable media device, you can create a backup of the removable media device's Sector 0 data, and when needed, use it to perform the recovery procedure outlined below.

Create this backup before you actually need it. If the device fails and you do not have the Sector 0 data, this recovery procedure cannot be performed.

Refer to page 86 for details on the recovery procedure.

This procedure should be performed **on each USB flash drive that is deployed**.

1. Insert the USB flash drive into a computer that does not have ProtectDrive installed, and make sure the device drive appears as a readable drive.
2. Run the **dskprobe.exe** utility. (This utility is included in the Microsoft Windows 2003 Resource Kit and can be downloaded from the Internet.)
3. Select **Drives > Physical Drive**.
4. Double-click the last drive in the list, which should be the USB flash drive. It will appear under **Handle 0** in the bottom of the screen.
5. Select **Set Active** for that drive, and then click **OK**.
6. Make no changes to the default settings. Select **Sectors > Read**, and then click **Read**. The Sector 0 data will be displayed.
7. Select **File > Save As**. Choose a secure location, such as a protected hard drive or network drive. Specify a filename that clearly identifies the device from which the data came.

Custom Recovery Key Set Creation

The **Certificate Wizard** utility (**certwizardapp.exe**) is used to create a custom recovery key set. Use the **Certificate Wizard** to create any or all of the following files:

- **Master Security Certificates (MSC)**—These **PdMaster.cer** and **PdMaster.pfx** files are used for Disk Key Recovery in the Remote Recovery Console (**rpadmin**). These certificates should be securely stored and only be accessible to individuals who can perform disaster recovery.

- **Recovery Support Certificates (RSC)**—These **PdRecovery.cer** and **PdRecovery.pfx** files are used for Emergency Logon in the Remote Recovery Console (**rpadmin**). These certificates should only be accessible to individuals who can perform password recovery (for example, Help Desk/Support personnel).

- **Salt**—This file is used to permit the sharing of removable media between ProtectDrive PCs.

The execution of the **Certificate Wizard** on Windows XP SP2 requires ProtectDrive to be installed on that system.

If you have already installed ProtectDrive and you want to create a custom recovery key set, make sure you copy the **PdMaster, PdRecovery,** and **salt** files that were created or used during the ProtectDrive installation, and save them to another location. Otherwise, these files may be overwritten. After you have safely stored these files to another location, follow the **Certificate Wizard** procedure on page 25.

If you have **not** installed ProtectDrive yet, and you want to use a custom recovery key set during the installation, follow the **Certificate Wizard** procedure on page 25 **before** you install ProtectDrive.

The **Certificate Wizard** utility is located in the *\Tools* directory on the ProtectDrive distribution CD.

© SafeNet, Inc.

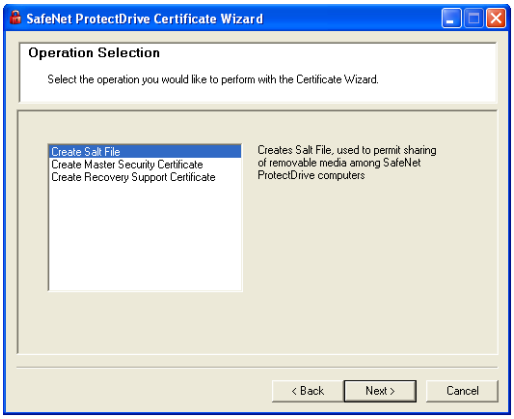
Certificate Wizard Procedures

Create a Salt File

This option is used to permit sharing of removable media among ProtectDrive computers.

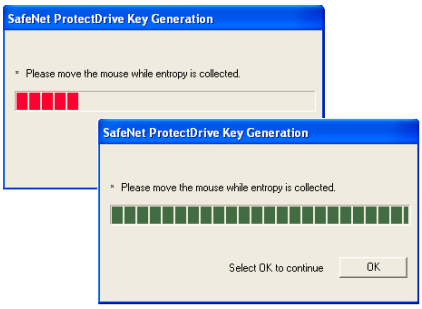
1. Navigate to the *\Tools* directory on the ProtectDrive distribution CD, and then double-click on **certwizardapp.exe**. When the **Certificate Wizard** displays, click **Next** to continue.

2. Double-click **Create Salt File**, or select the operation, and then click **Next**.


SafeNet ProtectDrive Certificate Wizard
Operation Selection
Select the operation you would like to perform with the Certificate Wizard.
Create Salt File
Create Master Security Certificate
Create Recovery Support Certificate
Creates Salt File, used to permit sharing of removable media among SafeNet ProtectDrive computers
< Back
Next >
Cancel

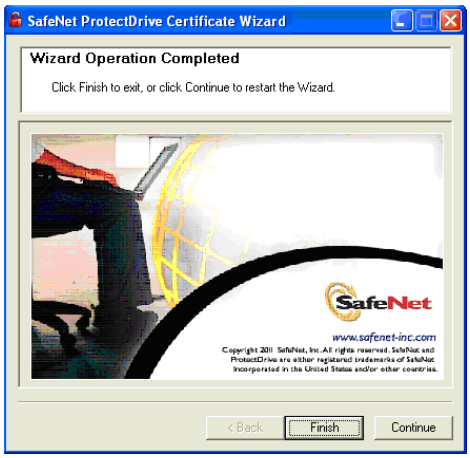
3. Browse to the directory where you want to save the output file, and then click **Next**.

4. The system will proceed to collect entropy to generate the recovery files. Move the mouse, and then click **OK** when it is completed.


SafeNet ProtectDrive Key Generation
Please move the mouse while entropy is collected.
SafeNet ProtectDrive Key Generation
Please move the mouse while entropy is collected.
Select OK to continue
OK

5. Click **Next**.

6. When the creation process is complete, the following screen displays. Click **Finish** to close the **Certificate Wizard**, or click **Continue** to return to the *Operation Selection* screen to perform another procedure.



7. Verify that the **Salt** file was created and saved to the location you specified in step 3.

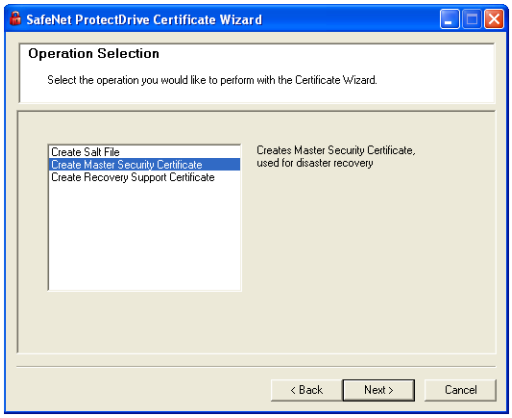
© SafeNet, Inc.

Create a Master Security Certificate

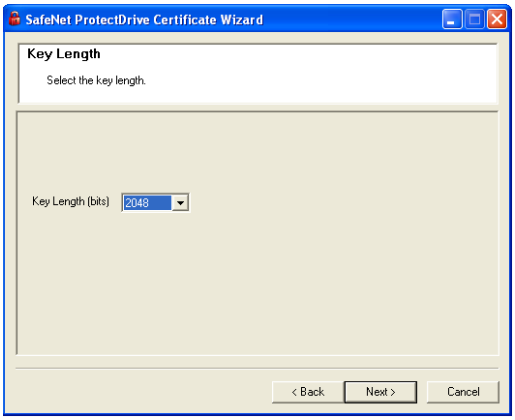
This option is used to create a Master Security Certificate to use for disaster recovery.

1. Navigate to the *\Tools* directory on the ProtectDrive distribution CD, and then double-click on **certwizardapp.exe**. When the **Certificate Wizard** displays, click **Next** to continue.

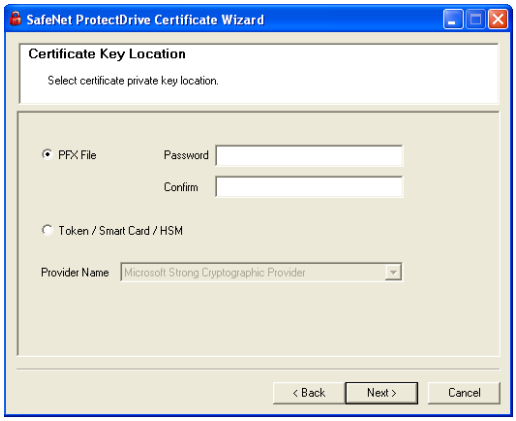
2. Double-click **Create Master Security Certificate**, or select the operation, and then click **Next**.


SafeNet ProtectDrive Certificate Wizard
Operation Selection
Select the operation you would like to perform with the Certificate Wizard.
Create Salt File
Create Master Security Certificate
Create Recovery Support Certificate
Creates Master Security Certificate, used for disaster recovery
< Back
Next >
Cancel

3. Select the **Key Length** and then click **Next**.



4. The following screen displays:



   - If you are creating a password-protected private key, select the **PFX File** option, enter and confirm the appropriate password, and then click **Next**.

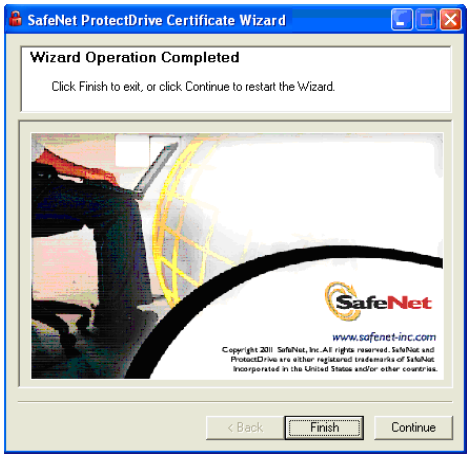
   - If you are creating a token- or smart card-based private key, select the **Token / Smart Card / HSM** option, choose the appropriate CSP from the **Provider Name** drop-down list, and then click **Next**.

5. Browse to the directory where you want to save the output file, and then click **Next**.

6. When the recovery files are successfully created, the following message displays. Click **Next** to continue.

© SafeNet, Inc.

7. When the creation process is complete, the following screen displays. Click **Finish** to close the *Certificate Wizard*, or click **Continue** to return to the *Operation Selection* screen to perform another procedure.



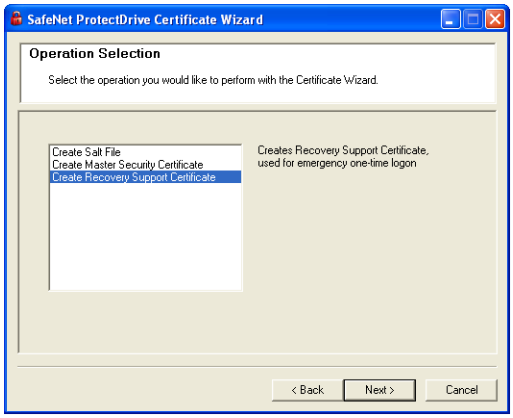
8. Verify that the **PdMaster** files were created and saved to the location you specified in step 5.

Create a Recovery Support Certificate

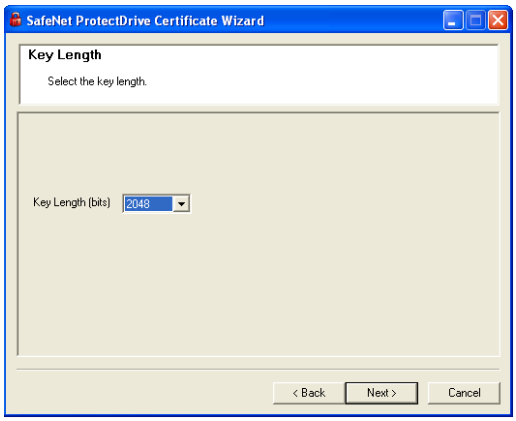
This option is used to create a Recovery Support Certificate to use for emergency one-time logon.

1. Navigate to the *\Tools* directory on the ProtectDrive distribution CD, and then double-click on **certwizardapp.exe**. When the *Certificate Wizard* displays, click **Next** to continue.

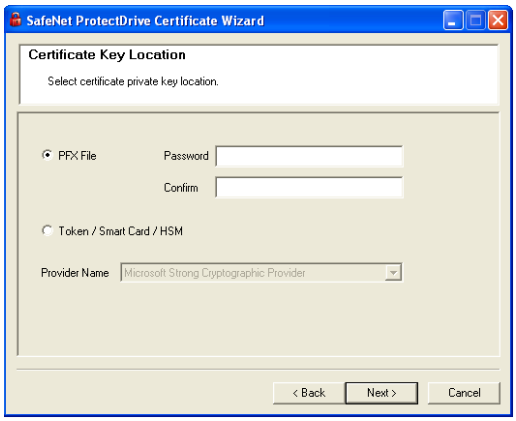
2. Double-click **Create Recovery Support Certificate**, or select the operation, and then click **Next**.


SafeNet ProtectDrive Certificate Wizard
Operation Selection
Select the operation you would like to perform with the Certificate Wizard.
Create Salt File
Create Master Security Certificate
Create Recovery Support Certificate
Creates Recovery Support Certificate, used for emergency one-time logon
< Back
Next >
Cancel

Select the **Key Length** of the cryptographic algorithm to use to create the certificate, and then click **Next**.



3. The following screen displays:



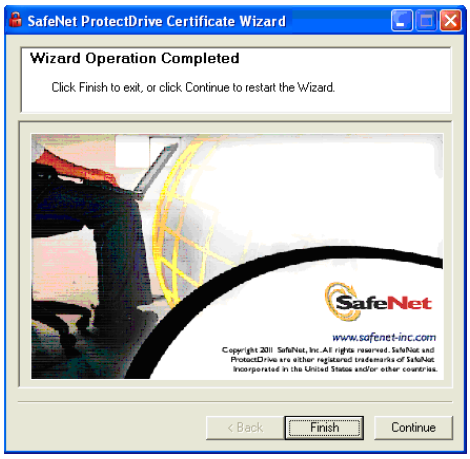
- If you are creating a password-protected private key, select the **PFX File** option, enter and confirm the appropriate password, and then click **Next**.
- If you are creating a token- or smart card-based private key, select the **Token / Smart Card / HSM** option, choose the appropriate CSP from the **Provider Name** drop-down list, and then click **Next**.

© SafeNet, Inc.

4. Browse to the directory where you want to save the output file, and then click **Next**.

5. When the recovery files are successfully created, the following message displays. Click **Next** to continue.

6. When the creation process is complete, the following screen displays. Click **Finish** to close the *Certificate Wizard*, or click **Continue** to return to the *Operation Selection* screen to perform another procedure.



7. Verify that the **PdRecovery** files were created and saved to the location you specified in step 5.

Remove ADAM Instance and Unused ADAM SCPs

In Active Directory environments, Active Directory Application Mode (ADAM) uses service connection points (SCPs) to publish ADAM service information in Active Directory.

An SCP is a pointer in Active Directory that contains information about a service (such as an ADAM instance), including how and where to contact that service. SCPs are important for ProtectDrive to locate the correct ADAM instance.

When an ADAM instance is removed from the computer, it deletes its SCP from Active Directory. If SCP removal fails, client applications may be directed to a nonexistent ADAM instance, which can cause the Active Directory server to be unresponsive.

There are several reasons why an SCP is not removed. Some possible causes are: Active Directory was unavailable during un-installation, or the SCP was created manually.

An SCP must be removed before a new ProtectDrive ADAM instance can be created, or before ProtectDrive can use Active Directory for storage. The procedure on page 33 requires the **ADSIEdit** utility to remove the ADAM SCP. Network administrators can use this utility to view and make changes to Active Directory. ADSIEdit features are similar to the Active Directory Users and Computers (ADUC) MMC snap-in, but the ADSIEdit utility provides a lower-level view of Active Directory information.

Install ADSI Edit

The ADSIEdit utility is included when Windows Server 2003 Support Tools are installed from the product CD. Alternatively, you can download ADSIEdit from the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=100114.

For details on how to install ADSI Edit on various operating systems, refer to the following Microsoft Web page:

http://technet.microsoft.com/en-us/library/cc773354(WS.10).aspx

For more information on ADAM SCPs, refer to the *Administering ADAM* service publication at:

http://technet.microsoft.com/en-us/library/cc736338(WS.10).aspx.

© SafeNet, Inc.

Remove the ADAM Instance

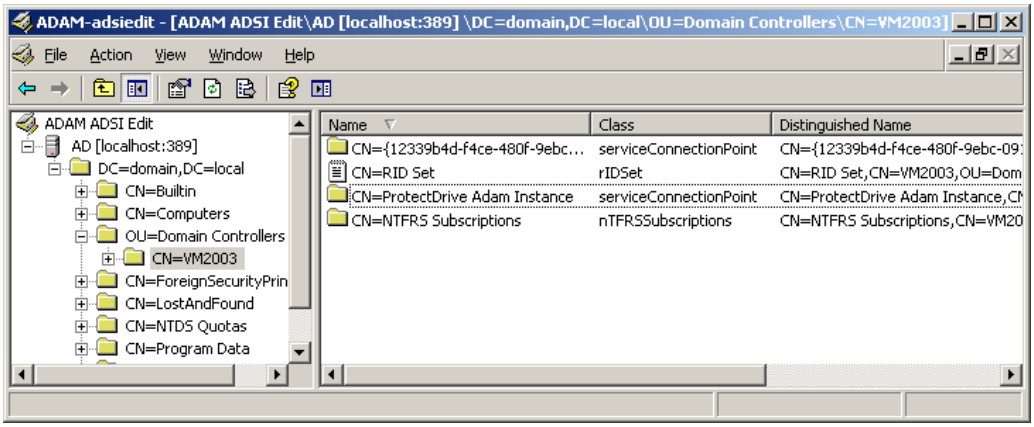
1. From the Windows *Start* menu, go to **Add/Remove Programs**.
2. Select **ADAM Instance ProtectDrive,** and then click **Remove**.

If the ProtectDrive ADAM instance has been replicated, make sure you select the correct instance to remove (*PD Instance, PD Instance1, PD Instance2, etc.*).

Remove the ADAM SCP

When an ADAM instance is removed, its SCP should be deleted from Active Directory. If SCP removal fails, follow the steps below.

1. Launch the **ADSIEdit.msc** utility in the MMC.
2. Connect to your Active Directory, and browse to the computer object that hosted the ADAM instance.

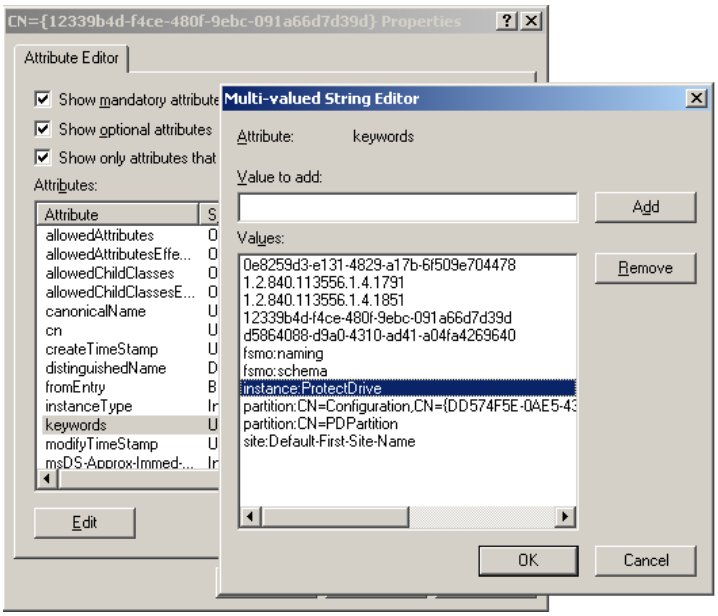


You will see one or more objects with a **serviceConnectionPoint** class. (There are two in the example shown above.)

3. Right-click on each of these objects to view their properties, select the **keywords** attribute, and then click **Edit**.

   - If you see the **instance:ProtectDrive** value listed for this attribute in the **Multi-valued String Editor** window, you have verified that this is the SCP for the ProtectDrive ADAM instance. Continue with step 4.

   - If you do **not** see the **instance:ProtectDrive** value listed for this attribute in the **Multi-valued String Editor**, this is an SCP for a different service. Do not delete or modify it.



4. After you have located the ProtectDrive SCP, close the **Multi-valued String Editor** and the **Attribute Editor** windows.

5. Select the ProtectDrive SCP to remove from the right pane in **ADSIEdit** and select **Action > Delete**.

6. Click **Yes** to confirm the deletion.

© SafeNet, Inc.

Configure the Windows Firewall for ADAM

To help protect the security of your ProtectDrive server and clients, you should keep Windows Firewall turned on. To ensure successful client updates when using ADAM, you'll need to configure the firewall to allow traffic over port 50000, which ProtectDrive uses to communicate to ADAM.

On the Server

1. Open the Windows *Control Panel*.
2. Select **Security Center > Windows Firewall**.
3. Click the **Exceptions** tab.
4. Click **Add Port**.
5. Enter the server's **Name**.
6. Enter the **Port number** on which the ADAM instance was created. For details on creating the ADAM instance, refer to page 47.
7. Click **OK**.

On Each Client

1. Open the Windows *Control Panel*.
2. Select **Security Center > Windows Firewall**.
3. Click the **Exceptions** tab.
4. Click **Add Program**.
5. Browse to *C:\Program Files\SafeNet ProtectDrive*.
6. Select **ClientDM**, and then click **Open**.
7. Click **OK**.

Enable ADAM or AD LDS on a Member Server

The ProtectDrive server can centrally manage its clients by using either Active Directory or ADAM. Please note the following:

- If you already have a member server running ADAM, or you plan to use Active Directory, skip this section and follow the domain preparation procedure on page 45.
- If you choose to use ADAM to centrally manage the ProtectDrive clients, follow the appropriate ADAM (or AD LDS) procedure on the following pages.
- If you are using Windows 2003 R2, then ADAM is already a part of the operating system, and you simply need to enable ADAM via **Add/Remove Components**, described in the *Enable ADAM* procedure on the next page.
- If you are not using Windows 2003 R2, you must first download an ADAM installation from Microsoft, and then follow the *Enable ADAM* procedure on the next page to enable it.
- If you are using Windows 2008 R2, then AD LDS is already a part of the operating system, and you simply need to enable AD LDS via **Server Manager**, described in the *Enable AD LDS* procedure on page 39.
- For a detailed overview of ADAM and AD LDS, refer to the following Microsoft Web pages:

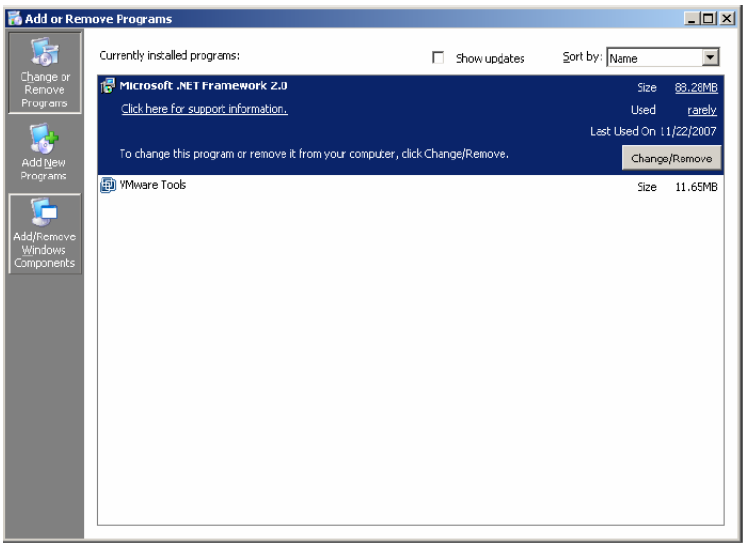
  http://technet.microsoft.com/en-us/library/cc776389(WS.10).aspx

  http://technet.microsoft.com/en-us/library/cc754361(WS.10).aspx

© SafeNet, Inc.

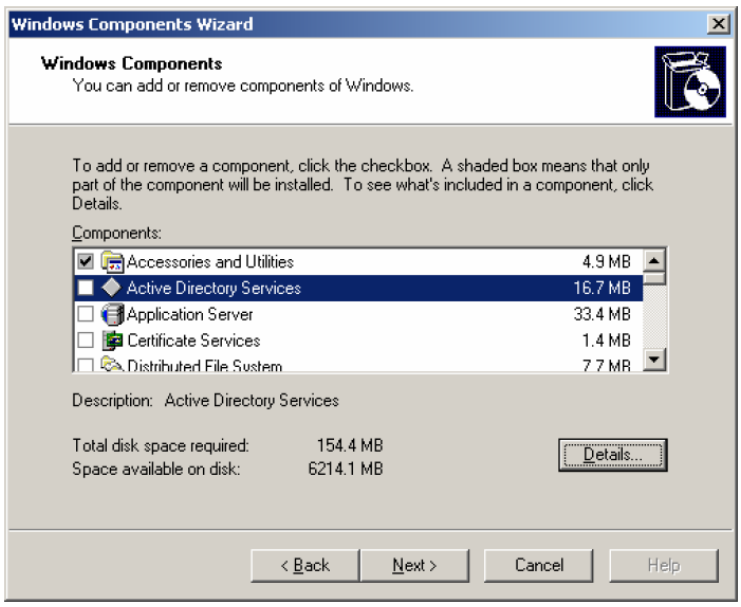
Enable ADAM

1. On the member server, select **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.



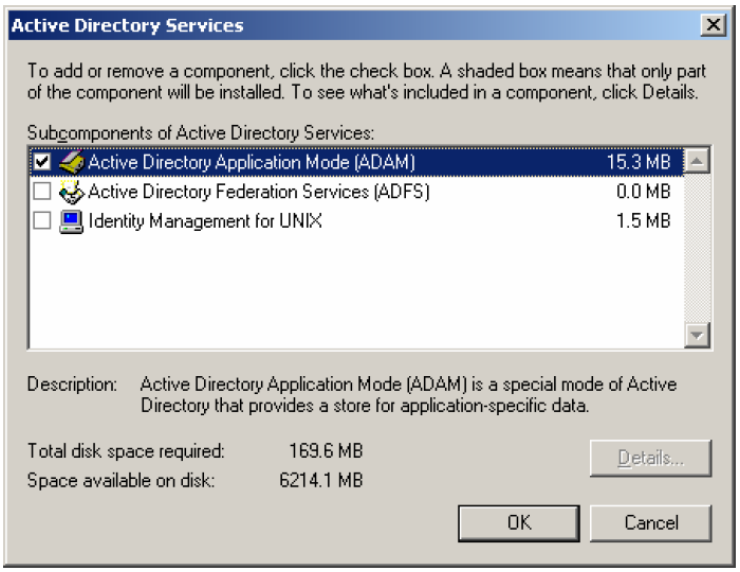
3. Highlight the **Active Directory Services** component.

Do not select the corresponding **Active Directory Services** check box. If this option is selected, additional subcomponents will be installed, which may cause errors.


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 4.9 MB
Active Directory Services 16.7 MB
Application Server 33.4 MB
Certificate Services 1.4 MB
Distributed File System 7.7 MB
Description: Active Directory Services
Total disk space required: 154.4 MB
Space available on disk: 6214.1 MB
Details...
< Back
Next >
Cancel
Help

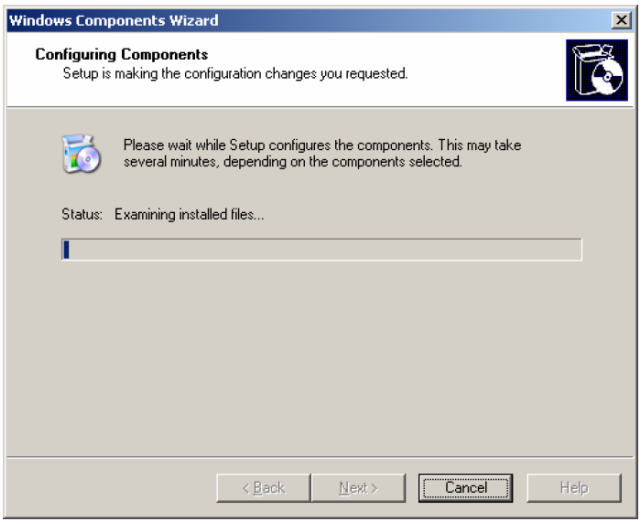
4. Click **Details**.

5. Select the **Active Directory Application Mode (ADAM)** check box. Do not select the other subcomponents.

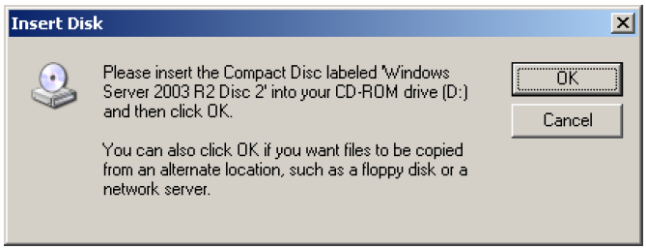

Active Directory Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Active Directory Services:
Active Directory Application Mode (ADAM) 15.3 MB
Active Directory Federation Services (ADFS) 0.0 MB
Identity Management for UNIX 1.5 MB
Description: Active Directory Application Mode (ADAM) is a special mode of Active Directory that provides a store for application-specific data.
Total disk space required: 169.6 MB
Space available on disk: 6214.1 MB
Details...
OK
Cancel

6. Click **OK**.

7. Click **Next**. The components will be installed.


Windows Components Wizard
Configuring Components
Setup is making the configuration changes you requested.
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.
Status: Examining installed files...
< Back
Next >
Cancel
Help

8. When prompted, insert the Windows Server 2003 R2 Disc 2, and then click **OK**.


Insert Disk
Please insert the Compact Disc labeled 'Windows Server 2003 R2 Disc 2' into your CD-ROM drive (D:) and then click OK.
You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.
OK
Cancel

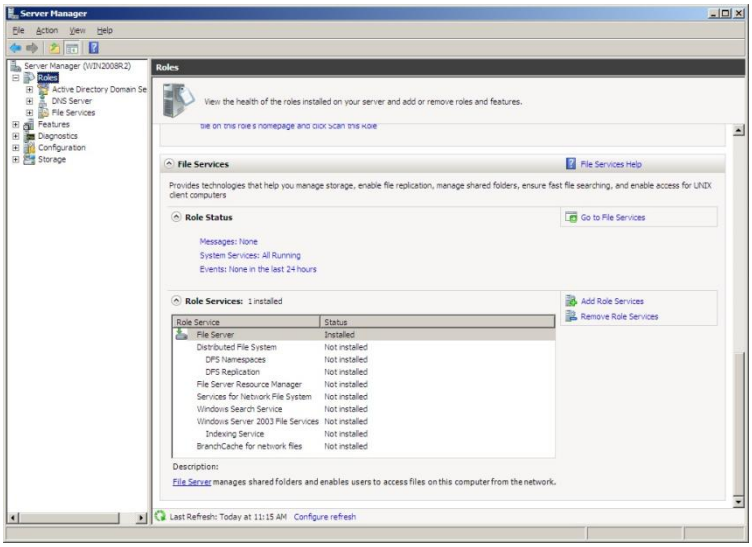
© SafeNet, Inc.

9. Click **Finish** to complete the procedure.

10. Proceed to *Prepare the Windows Domain* on page 45.

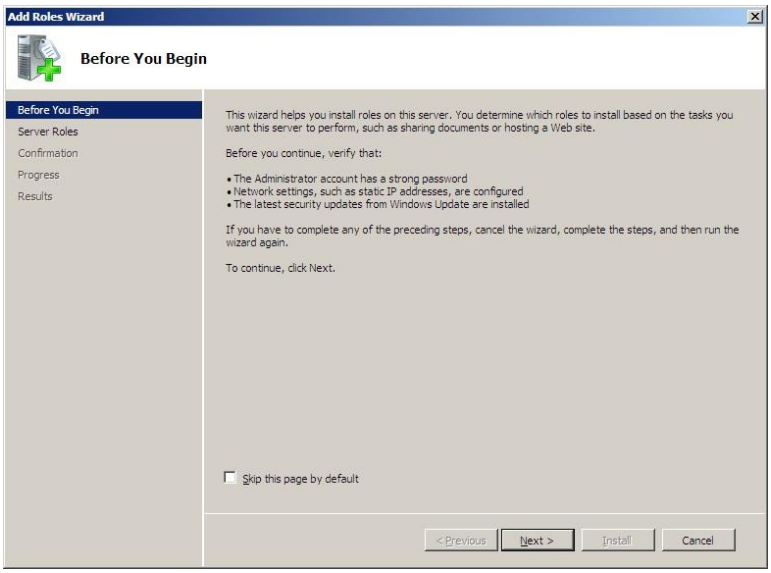
Enable AD LDS

1. On the member server, select **Start > Server Manager**.

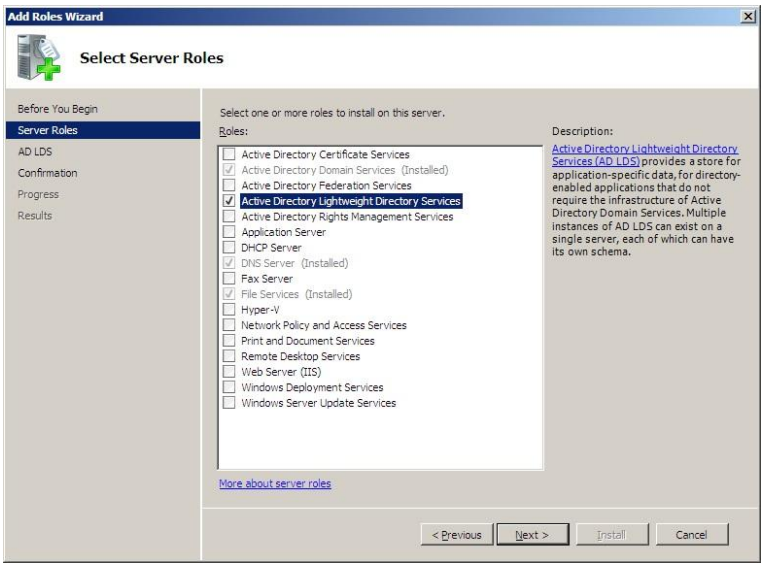


2. In the console tree, right-click **Roles**, and then click **Add Roles**.

3. Review the information on the **Before You Begin** page of the *Add Roles Wizard*, and then click **Next**.


Add Roles Wizard
Before You Begin
Before You Begin
Server Roles
Confirmation
Progress
Results
This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.
Before you continue, verify that:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The latest security updates from Windows Update are installed
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

4. On the **Select Server Roles** page, in the *Roles* list, select the **Active Directory Lightweight Directory Services** check box, and then click **Next**.


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
AD LDS
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server (Installed)
Fax Server
File Services (Installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description:
Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.
More about server roles
< Previous
Next >
Install
Cancel

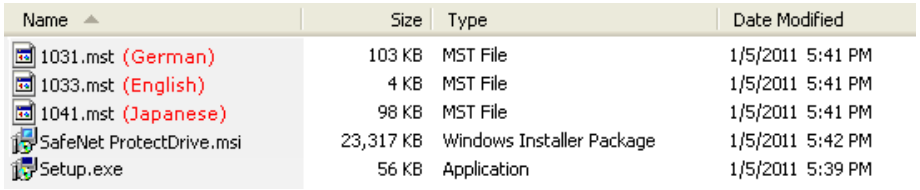
5. Follow the remaining instructions in the wizard and finish adding the AD LDS server role.

6. After the installation is finished, the **Installation Results** screen displays. Review the messages on the screen to ensure the installation was successful, and then click **Close**.

© SafeNet, Inc.

ProtectDrive Install (MSI) Package

ProtectDrive is deployed using a Windows Installer (MSI) package. The files shown below are used to install the ProtectDrive Administrative Management Tools and Client-side components.



Name	Size	Type	Date Modified
1031.mst (German)	103 KB	MST File	1/5/2011 5:41 PM
1033.mst (English)	4 KB	MST File	1/5/2011 5:41 PM
1041.mst (Japanese)	98 KB	MST File	1/5/2011 5:41 PM
SafeNet ProtectDrive.msi	23,317 KB	Windows Installer Package	1/5/2011 5:42 PM
Setup.exe	56 KB	Application	1/5/2011 5:39 PM

Additionally, an Active Directory Group Policy Object (GPO), responsible for software deployment, can be configured (customized) for network roll-out of the **SafeNet ProtectDrive.msi** to multiple client systems.

Alternatively, with ProtectDrive version 8.3 (and higher) it is possible to customize installations via the ProtectDrive Management Console Configuration Objects (see page 55).

If you are deploying ProtectDrive on a Windows 7, Windows Vista, or Windows Server 2008 client, run **Setup.exe** (located in the same directory) instead of **SafeNet ProtectDrive.msi**.

If deployment to a computer is via GPO, and there is an existing *<computer>_RecoveryEnvelope.env* file created by a previous manual installation of ProtectDrive from the same directory, then this .env file should be deleted or saved elsewhere.

Customizing the MSI Package

If silent installation is desired (GPO deployment, for example), the System Administrator must set all the required parameters of the **Property** to require no user interaction during installation. This may be achieved by modifying the MSI package.

MSI is a database table, and the System Administrators can tune, or customize, the **SafeNet ProtectDrive.msi**, as needed. There are a number of tools publicly available that can be used to customize the MSI package.

For example, Microsoft provides a free database editor called Orca. Refer to the following Web site for more information on Orca:

`http://support.microsoft.com/kb/255905/EN-US/ 1`

ProtectDrive MSI Properties

The MSI properties described below can be added (**if not already present in the .msi file**) and/or modified for a ProtectDrive installation.

ERA_CLIENT_CONFIGURATION_ONLY	This property defines the type of client configuration to install. Set it to (1) to configure the client locally via the **Local Management Console** (this will disable Active Directory/ADAM updates). Set it to (0) to remotely configure the client via Active Directory/ADAM on the server (this will disable local changes via the **Local Management Console**).
ERA_CONFIG_FILE_IMPORT_FLAGS	This property defines the XML file to import during the installation. Set it to (1) to only import users from the file specified in ERA_CONFIG_FILE_XML_PATH. Set it to (2) to only import data from the file specified in ERA_CONFIG_FILE_XML_PATH. Set it to (3) to import users and data from the file specified in ERA_CONFIG_FILE_XML_PATH.
ERA_CONFIG_FILE_XML_PATH	This property defines the absolute path that contains the **.xml file** of the ProtectDrive client configuration settings. This file can be imported to each client that shares the same salt.cid. The ProtectDrive installation looks for the **.xml** file in the current folder where **SafeNet ProtectDrive.msi** is located. Refer to page 91 for more on importing the client configuration .xml file.
ERA_ENCRYPT_USE_FIPS	This property is intended for use in upgrades only (to save/restore the FIPS flag during the upgrade). This property is set to (1) by default to use the FIPS-approved crypto. Set it to (0) to use the non-FIPS-approved crypto. If set to 0, performance is enhanced and a secure, Common Criteria EAL-4 approved, non-FIPS library is used.
ERA_INSTALL_AD_MC	This property is set to (0) by default. Set it to (1) to install the Active Directory/ADAM Computer Object snap-in, the Active Directory/ADAM User Object snap-in, and the ProtectDrive Management Console.

© SafeNet, Inc.

ERA_INSTALL_ADMIN_GUIDE	This property is set to (0) by default. Set it to (1) if you wish to install the *ProtectDrive Administration Guide*. To install this file, it must reside in the same directory as the MSI package.
ERA_INSTALL_CLIENT	This property is set to (1) by default. Set it to (0) to **not** install the Client component. This is also set to (1) automatically if **ERA_INSTALL_LOCAL_MC** is set to (1).
ERA_INSTALL_KEY_RECOVERY	This property is set to (0) by default. Set it to (1) to install **rpadmin.exe.** Refer to *Chapter 10 - Extraordinary Authentication Scenarios* for additional information.
ERA_INSTALL_LOCAL_MC	This property is set to (1) by default. Set it to (0) to **not** install the **Local Management Console** utility.
ERA_INSTALL_USER_MANUAL	This property is set to (1) by default. Set it to (0) to **not** install the *ProtectDrive User Manual*. To install this file, it must reside in the same directory as the MSI package.
ERA_KM_REC_FILES_FOLDER_PATH	This property defines the recovery file path (relative, full or network path) that contains the recovery file set. The default recovery file set path is the source directory (from which the **SafeNet ProtectDrive.msi** file is run).
ERA_LANGUAGE_CHOICE	This property defines the language used for labels and text messages. It is set to the operating system language by default (0). Alternate settings are: (1) English, (2) German, or (3) Japanese.

ERA_LICENSE_PATH_OR_CODE	This property **does not** exist in the **SafeNet ProtectDrive.msi** file by default. This property defines the license path (relative, full or network path) that contains the ProtectDrive license file, or the full license code (copied/pasted from the license.txt file). The default license file path is the source directory (from which the **SafeNet ProtectDrive.msi** file is run). If this property is not defined, then the installation searches for a **license.txt** file. If **authorization.txt** also exists, then it will take precedence over **license.txt**. If neither file exists, then the trial license is installed.
ERA_NO_NETBSD	This property applies to upgrades only (32-bit pre-boot installation is the default). If a legacy 16-bit installation is desired, set this property to (1). If set to (1), the **ERA_VROM_READERS_SET** property must also be set. If a 32-bit environment is already installed and there is a need to revert to legacy 16-bit, press the **[Shift]** key while the PC is booting. The PC will start in 16-bit pre-boot one time only (until the next reboot occurs). To make this adjustment permanent, please contact Technical Support.
ERA_SETUP_TYPE	This property is set to **Client** by default for client installation. Set to **Server** to install Administrative Management Tools (ProtectDrive Management Console, PDDirPrep, Remote Recovery Console, etc).
ERA_VROM_READERS_SET	This property applies to 16-bit pre-boot installations only. Due to driver limitations in the 16-bit pre-boot environment, it is necessary to identify which groups of smart card readers are required. (32-bit installations include support for all readers.) This property defines the readers supported at pre-boot authentication. This property is set to **INTERNAL** by default. Set to **PCMCIA** to install PCMCIA supported readers. If none are required, do not change the default setting.

© SafeNet, Inc.

Deploying Administrative Management Tools

How has the ProtectDrive Installation Changed?

If you are familiar with ProtectDrive versions prior to 8.3, you may find this information helpful. Otherwise, skip this section.

Prior to version 8.3, ProtectDrive included a **Typical Server Installation** option. As part of the ProtectDrive server installation process, this installation option would extend the schema and configure the server—all on the same computer.

In version 8.3 (and higher), the **Typical Server Installation** option was replaced with the **Administrative Management Tools Installation** option.

The ProtectDrive client installation did not change. Refer to page 64 for details.

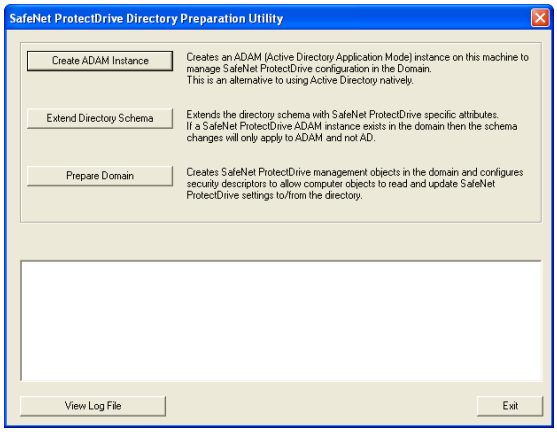
Install Administrative Management Tools wherever you intend to manage ProtectDrive from. The tools can be installed anywhere, and as many times as needed.

Administrative Management Tools are necessary to centrally manage ProtectDrive clients, perform disaster key recovery and emergency logon procedures. Refer to page 55 for more information on these tools.

Prepare the Windows Domain

The **Directory Preparation Utility** (**PDDirPrep**) is used to prepare the Windows domain for ProtectDrive. **PDDirPrep** is used to create a unique ADAM instance (and replicas of the ADAM instance) with a signed Master Security Certificate, extend the Active Directory or ADAM schema, and prepare the domains to remotely manage the ProtectDrive clients.

Run the PDDirPrep utility prior to running the ProtectDrive **Administrative Management Tools Installation**. Otherwise, the management tools will report errors (such as *Object Not Found*) until PDDirPrep has been used to prepare the domain.


SafeNet ProtectDrive Directory Preparation Utility
Create ADAM Instance
Creates an ADAM (Active Directory Application Mode) instance on this machine to manage SafeNet ProtectDrive configuration in the Domain.
This is an alternative to using Active Directory natively.
Extend Directory Schema
Extends the directory schema with SafeNet ProtectDrive specific attributes.
If a SafeNet ProtectDrive ADAM instance exists in the domain then the schema changes will only apply to ADAM and not AD.
Prepare Domain
Creates SafeNet ProtectDrive management objects in the domain and configures security descriptors to allow computer objects to read and update SafeNet ProtectDrive settings to/from the directory.
View Log File
Exit

It is only necessary to run PDDirPrep once per forest (to extend the directory schema) and once per domain (to prepare the domain). However, there is no harm in running it more than once—it will simply verify that all changes have been made, and make any that still need to be made (i.e., if a failure was encountered the first time PDDirPrep was run).

There are a few ways to launch **PDDirPrep**:

- Initially, you will access the utility from the ProtectDrive installation CD. Navigate to the *\Tools* directory and double-click on **PDDirPrep.exe**.
- After you have installed the **Administrative Management Tools**, you can also access PDDirPrep using one of these methods:
  - At the end of the ProtectDrive installation—Select the **Launch Directory Preparation Utility** check box on the final installation screen, and the utility will start after the installation is complete.
  - From the Windows Start menu—Select **Start > Programs > SafeNet ProtectDrive > Directory Preparation Utility**.

PDDirPrep consists of the following tasks:

- **Create ADAM Instance**
- **Extend Directory Schema**
- **Prepare Domain**
- **View Log File**

Perform the first three tasks in the order in which they are listed above. Proceed to the next page for details on how to complete each task. You can view the log file any time.

After you have completed each PDDirPrep task, install the ProtectDrive Administrative Management Tools, as described on page 51.

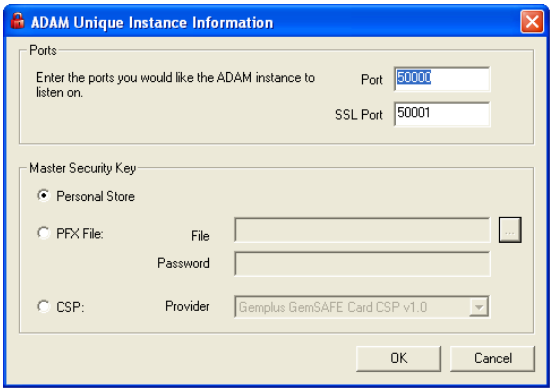
© SafeNet, Inc.

Create a Unique ADAM Instance

Perform this task if you need to create a unique ProtectDrive ADAM instance. It must be created on a computer that is not a domain controller running Active Directory. Each domain can contain one ADAM configuration set, which consists of the unique ProtectDrive ADAM instance and its replicated instances.

After the unique ProtectDrive ADAM instance is created, you can create one or more replicas of the ADAM instance as a backup. Refer to page 48 for details.

1. Click **Create ADAM Instance**.



2. Enter the **Port** and **SSL Port** values on which to create the ADAM instance.

3. Select the appropriate **Master Security Key** option:

   - **Personal Store**—If you select this option, the Master Security Certificate's private key must be in the user's Personal Certificate Store on this machine.

   - **PFX File**—If you select this option, click ..., browse to the **PdMaster.pfx** file, and then enter the password.

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

4. Click **OK**. The status window displays the action(s) being performed. Information is also logged to the PDDirPrep log file.

5. Proceed to the **Extend Directory Schema** task.

Create a Replica of the ADAM Instance

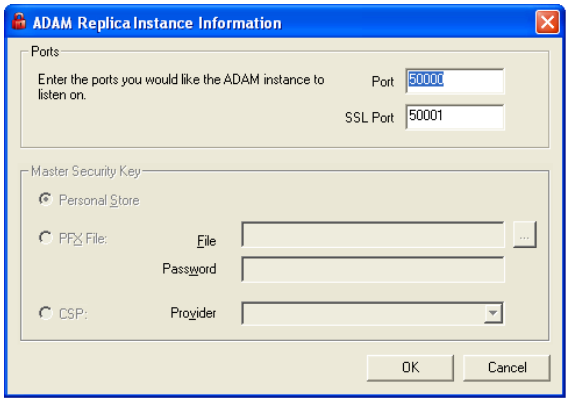
After the unique ProtectDrive ADAM instance is created, you can create one or more replicas of the ADAM instance. A replica of an ADAM instance uses duplicate configuration and schema partitions from the unique ADAM instance. Computers with the ADAM replica connect to the unique ADAM instance using the same ports. Any configuration changes made to the primary (unique) ADAM instance will be updated on the replica(s).

Having an ADAM replica always ensures there is a backup available. In the event the primary ADAM server is inaccessible, the clients can continue to be updated via the replicated (secondary) ADAM instance until the primary ADAM server is available again.

To view all of the configurations, simply open the **ProtectDrive Management Console** on the secondary server. If multiple instances were created, the clients will continue to search for an accessible ADAM replica instance (in random order) until one is located. Replicas are named sequentially—the unique ADAM instance is named *PD Instance*, so the first replica is named *PD Instance1*, the second is named *PD Instance2*, and so on.

Follow the steps below to create the replica(s) of the primary ADAM server instance on another member server in the same domain. In this procedure, note that the **Master Security Key** options are inactive, as it is replicated from the unique ADAM instance.

1. Click **Create ADAM Instance**.



2. Enter the **Port** and **SSL Port** values on which to create the ADAM replica.

3. Click **OK**. The status window displays the action(s) being performed. Information is also logged to the PDDirPrep log file.

© SafeNet, Inc.

About Replication Delays

Replication takes time. You may find that configuration changes do not immediately propagate to the clients if they are pulling updates from a replicated ADAM instance. Be patient. Depending on the configuration, it can take several seconds, up to several minutes. Generally, this may be an issue when you are making configuration changes on the newly recovered unique instance, while at the same time, the clients are pulling updates from the replica instance that was previously in control.

If you are experiencing replication issues, determine whether an instance is –bindable." Use ADAM ADSIEdit and try to connect to the node with DN –CN=PDPartition" on the instance being tested. If the connection fails, then most likely, the PDMC and ProtectDrive clients will fail too, when trying to bind to this instance. Wait a few minutes, and then check that the clients have been updated with the configuration changes.

Extend Directory Schema

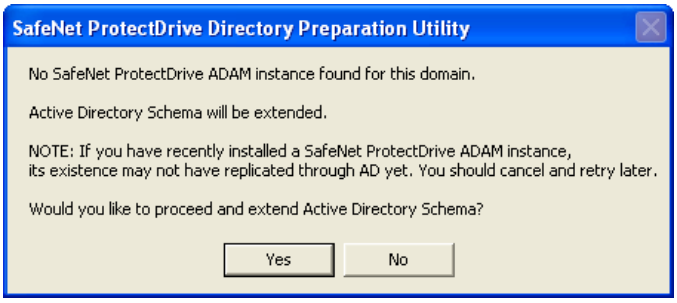
You must be a member of the *Schema Admins* group to perform this task. Perform this task to extend the Active Directory or ADAM schema to include attributes needed for ProtectDrive data storage.

For Active Directory, extend the directory schema on the primary domain. It is automatically replicated to all child domains. Only Active Directory schema changes are forest-wide.

If ADAM is being used, this task cannot be performed until an ADAM instance has been created on the domain.

1. Click **Extend Directory Schema**.

2. The system will verify whether an ADAM configuration set exists. If one exists, then the unique ADAM instance is extended. If one does **not** exist, then the user (administrator) is prompted to confirm the extension of the Active Directory schema. If this prompt displays, click **Yes** to continue.


SafeNet ProtectDrive Directory Preparation Utility
No SafeNet ProtectDrive ADAM instance found for this domain.
Active Directory Schema will be extended.
NOTE: If you have recently installed a SafeNet ProtectDrive ADAM instance,
its existence may not have replicated through AD yet. You should cancel and retry later.
Would you like to proceed and extend Active Directory Schema?
Yes
No

3. The status window displays the action(s) being performed. Information is also logged to the PDDirPrep log file.

4. Proceed to the **Prepare Domain** task.

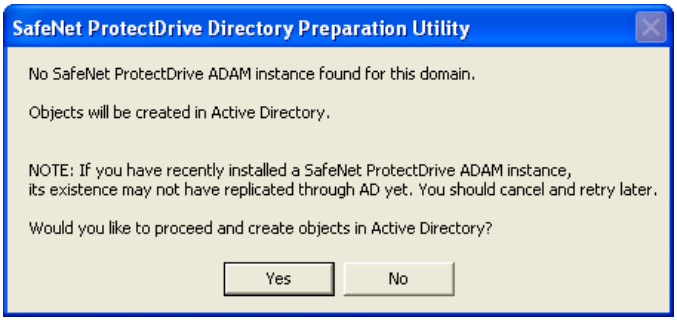
Prepare Domain

You must be logged in as the domain administrator to perform this task. This task prepares the Active Directory/ADAM domain objects for ProtectDrive data storage by attaching ProtectDrive attributes to existing computer objects, creating Default Configuration Objects, etc.

By default, all new clients in the domain will automatically be linked to the Default Configuration Object. (If you are upgrading from an earlier version of ProtectDrive, any existing clients will initially be managed by the property sheet of their own computer object. They will not automatically be linked to the *Default Configuration Object*, but can be linked to it later. Refer to page 59 for details on clients managed by the property sheet of their computer object.

1. Click **Prepare Domain**.

2. The system will verify whether an ADAM configuration set exists. If one exists, then the ADAM instance is configured with the domain directory changes. If one does **not** exist, then the user (administrator) is prompted to confirm the domain directory changes should be made to Active Directory. If this prompt displays, click **Yes** to continue.


SafeNet ProtectDrive Directory Preparation Utility
No SafeNet ProtectDrive ADAM instance found for this domain.
Objects will be created in Active Directory.
NOTE: If you have recently installed a SafeNet ProtectDrive ADAM instance,
its existence may not have replicated through AD yet. You should cancel and retry later.
Would you like to proceed and create objects in Active Directory?
Yes
No

3. The status window displays the action(s) being performed. Information is also logged to the PDDirPrep log file.

View Log File

You can view the log file any time. Use this file as an investigative tool for troubleshooting purposes.

As each task is performed, the status window will display information related to the action, and whether or not the action was successful. If the previous task has not been performed (or it has not completed), an error will display. All task-related information is also written to the log file.

1. Click **View Log File**. The file opens in Microsoft® Notepad.

2. Click **File > Exit** to close the file.

© SafeNet, Inc.

Install the ProtectDrive Administrative Management Tools

Before you begin, please note the following:

- If you intend to use ADAM with ProtectDrive, install ADAM on a machine (Windows Server 2003) that is not a domain controller running Active Directory. In addition, make sure ADAM is installed *prior* to installing and using the ProtectDrive tools.

- Run the **PDPrepDir** utility *before* you install the Administrative Management Tools (see page 45).

- Install the **ISSetupPrerequisites** *before* you install the ProtectDrive Administrative Management Tools (see below). These tools (located in the *\ISSetupPrerequisites* directory on the ProtectDrive distribution CD) are required to run ProtectDrive Management Console reports. If these prerequisites are not installed first, the ProtectDrive installation will fail. The *\ISSetupPrerequisites* directory includes the following subfolders:

Subfolder	Action Required
{074EE22F-2485-4FED-83D1-AAC36C3D9ED0}	Run **dotnetfx35.exe**. This is the .NET Framework 3.5 Setup.
{a0689fe9-3467-4d73-bc25-d0f696ad268a} **{cdd854f9-a31f-4f99-82f5-3c0be21104a4}**	Run **CRRedist2008_x86.msi** for a 32-bit environment. -OR- Run **CRRedist2008_x64.msi** for a 64-bit environment.

- Install the **ProtectDrive Administrative Management Tools** component *before* you install the client components. These tools are required to manage remote clients. Refer to page 55 for a description of each tool and how and when to use them.

1. Open the **ISSetupPrerequisites** folder and run **dotnetfx35.exe**. Then:

    - For 32-bit environments, run **CRRedist2008_x86.msi**.

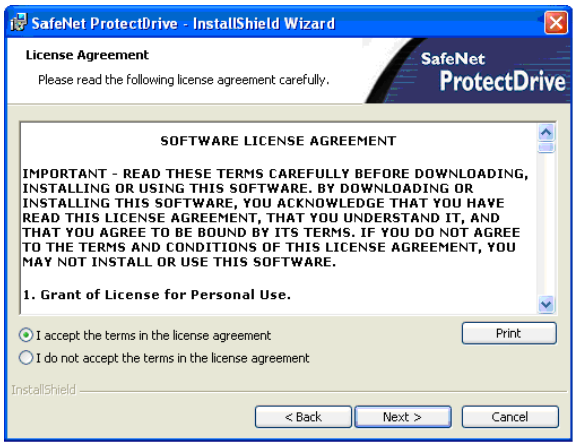
    - For 64-bit environments, run **CRRedist2008_x64.msi**.

2. Launch the **SafeNet ProtectDrive.msi**. The ProtectDrive installation wizard opens.

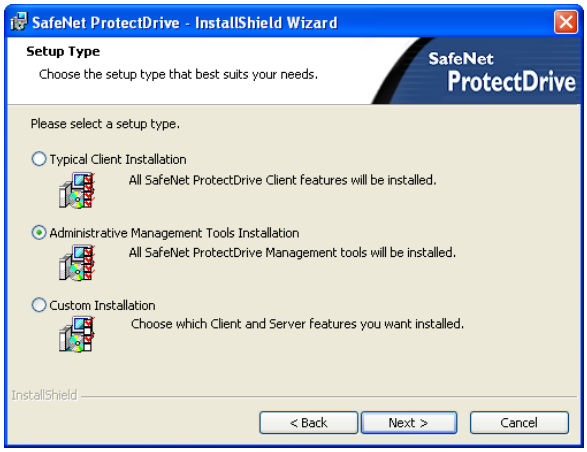
3. When the **Welcome** screen displays, click **Next**.

SafeNet ProtectDrive - InstallShield Wizard
Welcome to the InstallShield Wizard for SafeNet ProtectDrive
The InstallShield(R) Wizard will install SafeNet ProtectDrive on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
SafeNet
ProtectDrive
< Back
Next >
Cancel

4. Accept the **License Agreement**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SafeNet
ProtectDrive
SOFTWARE LICENSE AGREEMENT
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.
1. Grant of License for Personal Use.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

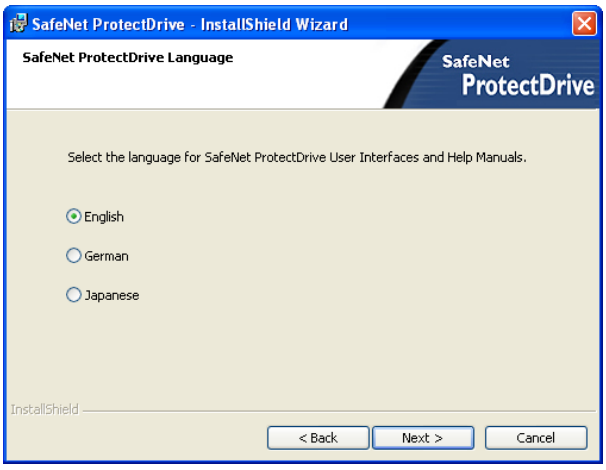
5. Select **Administration Management Tools Installation**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
SafeNet
ProtectDrive
Please select a setup type.
Typical Client Installation
All SafeNet ProtectDrive Client features will be installed.
Administrative Management Tools Installation
All SafeNet ProtectDrive Management tools will be installed.
Custom Installation
Choose which Client and Server features you want installed.
InstallShield
< Back
Next >
Cancel

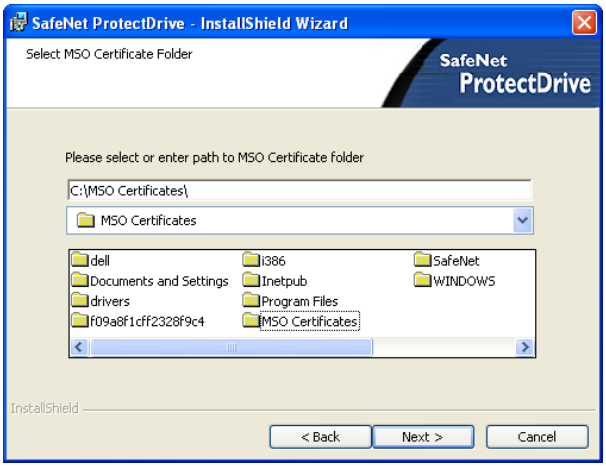
This selection will install the tools that are necessary to centrally manage ProtectDrive clients and perform disaster key recovery and emergency logon procedures.

© SafeNet, Inc.

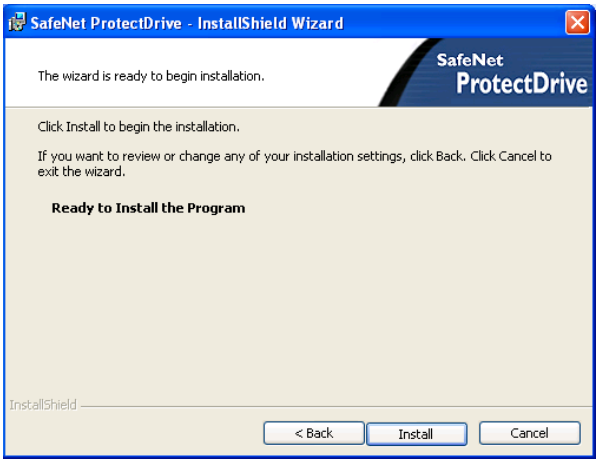
6. Select the language to be used for interface labels and text messages, and then click **Next**.



7. Browse to the MSO certificate folder where existing MSO certificates are located, and then click **Next**. This certificate ensures that a server or client will connect to an ADAM instance that has a Service Connection Point (SCP) with a signed MSO value.



8. The following screen displays. Click **Install** to continue.


SafeNet ProtectDrive - InstallShield Wizard
The wizard is ready to begin installation.
SafeNet
ProtectDrive
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Ready to Install the Program
InstallShield
< Back
Install
Cancel

9. When the installation is complete, the following screen displays.

- Leave the **Launch Directory Preparation Utility** check box enabled if you want PDDirPrep to run immediately after the installation is complete. Refer to the next section for more information on this utility.

- De-select the **Launch Directory Preparation Utility** check box if you do not want PDDirPrep to run immediately after the installation is complete.

10. Click **Finish**.

When the installation completes, a shortcut named **ProtectDrive Management Console** is added to the Windows desktop.

© SafeNet, Inc.

What are the ProtectDrive Administrative Management Tools?

Make sure you have configured the schema and domain by using **Directory Preparation Utility** (PDDirPrep) prior to installing the Administrative Management Tools. Otherwise, errors will occur when they are run (such as ―object not found" or ―attribute does not exist").

The ProtectDrive Administrative Management Tools are used to centrally manage ProtectDrive clients and perform disaster key recovery and emergency logon procedures. They can be installed on a machine that supports Active Directory, or via ADAM on a Windows Server 2003 machine which is not a domain controller.

Administrative Management Tools consist of:

- **ProtectDrive Management Console—**The **ProtectDrive Management Console** is used to centrally manage ProtectDrive clients. The console includes these snap-ins: **ProtectDrive Management**, which is used to create and manage multiple *Configuration Objects* for groups of ProtectDrive clients, **ProtectDrive Reports**, which is used to run Status and User reports, and **Active Directory Users and Computers** MMC. The ProtectDrive Management Console is described in more detail in the next section.

- **Remote Recovery Console—**The **Remote Recovery Console** is used to perform disaster key recovery and emergency logon procedures, and is discussed in Chapter 11.

- **Directory Preparation Utility (PDDirPrep)—**The **Directory Preparation Utility** is used to initially prepare a domain to remotely manage the ProtectDrive clients. It is provided here as part of the tool set as a convenience. PDDirPrep is also located on the ProtectDrive installation CD, in the *\Tools* directory, which is where you would typically run it. For details on this utility, refer to the *Prepare the Windows Domain* procedure on page 45.

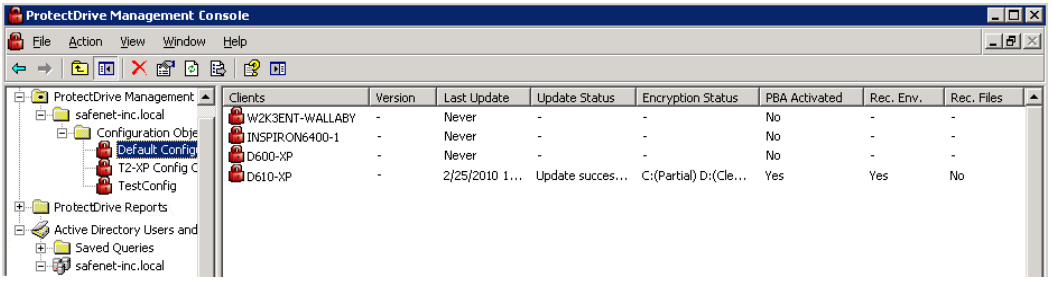
ProtectDrive Management Console

The following sections describe the suggested order in which to create new configuration objects and link clients to them. New configuration objects can only be added through the **ProtectDrive Management** snap-in in the ProtectDrive Management Console.

You can access the **ProtectDrive Management Console** two ways:

- From the Windows desktop, double-click the **ProtectDrive Management Console** shortcut icon. The shortcut is added to the Windows desktop during the ProtectDrive Administrative Management Tools Installation.

➢ From the Windows **Start** menu, select **Programs > SafeNet ProtectDrive > Management Console**.



If a client is managed by the property sheet of its own computer object (it relies on its own configuration which is automatically replicated from/to Active Directory or ADAM), use the **Active Directory Users and Computers** (ADUC) MMC snap-in instead. Refer to *Computer Object-managed Clients vs. Configuration-managed Clients* on page 59.

What are Configuration Objects?

A *Configuration Object* is a ProtectDrive policy that computers can be assigned to. By default, all remote clients will initially get their policy from the *Default Configuration Object*.

Prior to ProtectDrive version 8.3, remote clients were only managed through the ADUC MMC *Default Configuration Object*, meaning, only one ProtectDrive policy could be implemented per domain.

In version 8.3 (and higher), you can create multiple policy *Configuration Objects* and assign specific computers to them through the **ProtectDrive Management Console**. When computers are assigned to a particular configuration object, they will only receive the updates and changes made to the configuration to which they are linked.

Clients can still be managed individually through the ADUC snap-in, just as they have been in previous versions of ProtectDrive. Refer to *Computer Object-managed vs. Configuration-managed Clients* on page 59. A client managed by the property sheet of its own computer object can be assigned to a different *Configuration Object* at any time.

© SafeNet, Inc.

Create a New Configuration Object

1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Right-click on the **Configuration Objects** directory.
4. Select **New Configuration**.
5. Enter a name for the new configuration object, and then click **OK**. Do not use special characters (for example, —,” or —?”) in the name.
6. Proceed to the next section to add at least one user to the new configuration object.

Add a User to the New Configuration Object

Any time you add a new configuration object, make sure there is at least one user assigned to the configuration before making changes to the ProtectDrive settings.

1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Expand the **Configuration Objects** directory.
4. Right-click on the configuration object, and then select **Properties**.
5. Click the **PD Users** tab.
6. Click **Add**, and then follow the prompts to add a user.
7. Click **Apply**, and then click **OK**.
8. Proceed to the next section to modify the ProtectDrive settings for the configuration object.

Customize the New Configuration Object

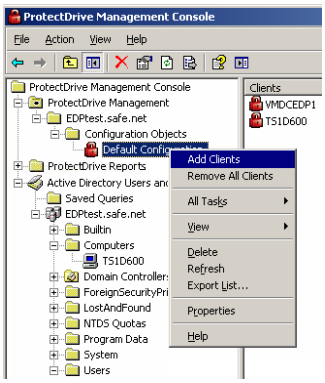
1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Expand the **Configuration Objects** directory.
4. Right-click on the configuration object, and then select **Properties**.
5. Click the **PD Settings** tab.

6. Customize the settings as needed for this configuration.
7. Click **Apply**, and then click **OK**.

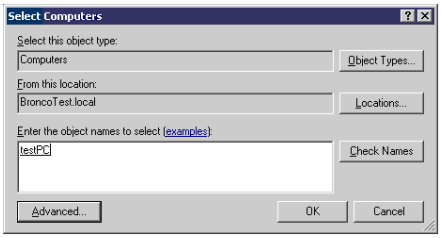
Assign a ProtectDrive Client to the New Configuration Object

A client can be assigned to a new or different configuration object at any time. Use this procedure to assign remote ProtectDrive clients to a configuration object other than the *Default Configuration Object*.

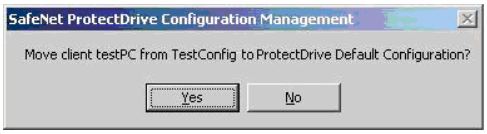
1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Expand the **Configuration Objects** directory.
4. Right-click on the configuration object, and then select **Add Clients**.



5. Locate the client to add, and then click **OK**.



6. Click **Yes** to confirm the addition of the selected client.



If the client you selected was already assigned to a different configuration, a confirmation prompt (similar to the one shown below) will display to confirm the move from one configuration assignment to another.

© SafeNet, Inc.

Remove a ProtectDrive Client from a Configuration Object

A client can be removed from a configuration at any time. When it is removed from a configuration, the client automatically reverts to being managed by the property sheet of its own computer object, and it can only be viewed in the **Active Directory Users and Computers** MMC snap-in.

You can reassign a client from being managed by the property sheet of its own computer object to a different configuration object (and vice-versa) any time. Refer to the next section for details on computer object-managed clients.

1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Click on the configuration object where the client to be removed is located.
4. Choose one of the following removal methods:
   - To *remove a single client*, right-click on the client to remove, and then select **Remove**.

     This method will revert the client to being computer object-managed.
   - To *remove all clients* in the configuration object, right-click on the configuration object, and then select **Remove All Clients**.

     A configuration object cannot be deleted when clients are still assigned to it.
5. Click **Yes** to confirm the action.

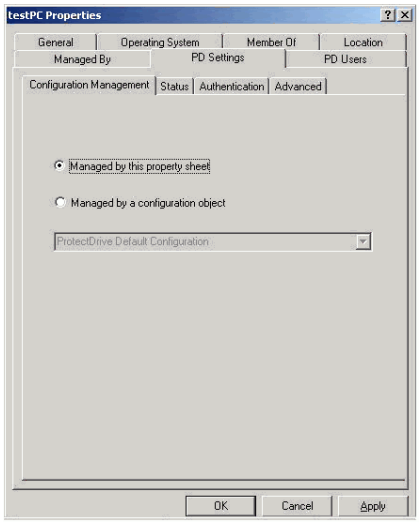
Computer Object-managed Clients vs. Configuration-managed Clients

When a client is computer object-managed, it relies on its own property sheet configuration, which is automatically replicated from/to Active Directory or ADAM. Computer object-managed clients can only be viewed in the **Active Directory Users and Computers** MMC snap-in.

Alternatively, a client managed by a different configuration object (other than its own configuration) is a configuration-managed client. You can reassign a client from being managed by its computer object, to a different configuration object (and vice-versa) any time. Refer to page 60 for details.

Change a Computer Object-managed Client to a Configuration Object-managed Client

1. On the server, open the **ProtectDrive Management Console**.
2. Open the **Active Directory Users and Computers** MMC snap-in.
3. Select **Computers**, right-click on the client, and then select **Properties**.
4. Select **PD Settings > Configuration Management**. The client will display as **Managed by this property sheet**.



5. Click **Managed by a configuration object**, and then select the desired configuration object from the drop-down list.
6. Click **Apply**, and then click **OK**. Note that the client no longer displays in **Active Directory Users and Computers**—it is now linked to the new client configuration object, and can only be viewed in the **ProtectDrive Management** snap-in.

Change a Configuration Object-managed Client to a Computer Object-managed Client

By simply removing the client from its currently assigned configuration object, the client will revert to being managed by its own property sheet configuration.

1. On the server, open the **ProtectDrive Management Console**.
2. Expand the **ProtectDrive Management** directory.
3. Expand the **Configuration Objects** directory.
4. Right-click on the client to reassign, and then click **Remove**.
5. Click **Yes** to confirm the action.

© SafeNet, Inc.

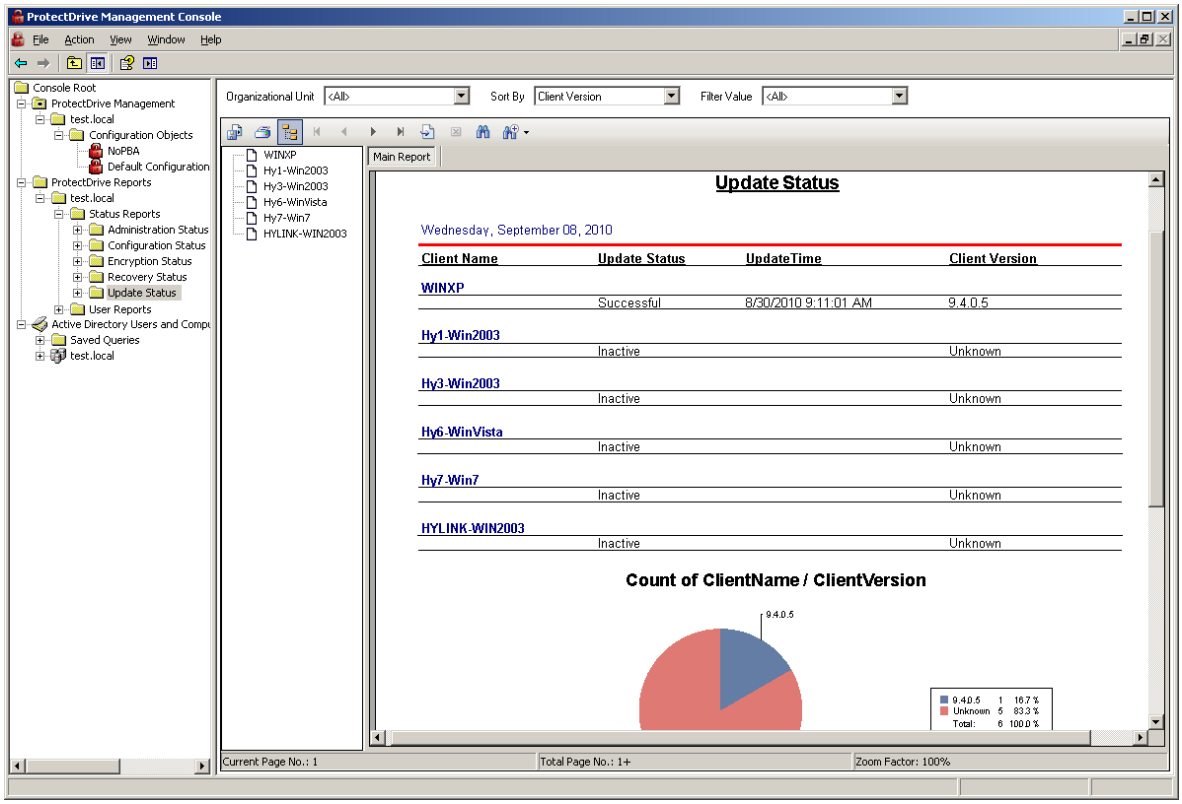
ProtectDrive Management Reports

Two installation prerequisites are required to run ProtectDrive Management Console reports. These prerequisites are located in the *\ISSetupPrerequisites* directory on the ProtectDrive distribution CD, and must be installed *before* you install the ProtectDrive Administrative Management Tools. Refer to page 51 for details.

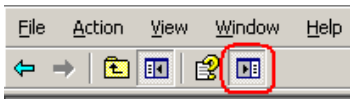
During the ProtectDrive **Administrative Management Tools Installation**, a **ProtectDrive Reports** snap-in is installed. This snap-in provides several built-in *Status* and *User* reports which can be run from the ProtectDrive Management Console (PDMC).

A domain administrator can run these reports any time, and view the state of the ProtectDrive clients in a domain. Report data can be viewed by Organizational Unit and sorted by various filtering criteria, printed, or exported.

Each report provides data in column format and includes a pie chart at the bottom of the report which represents percentages of the report data. An example of the *Update Status* report is shown below.

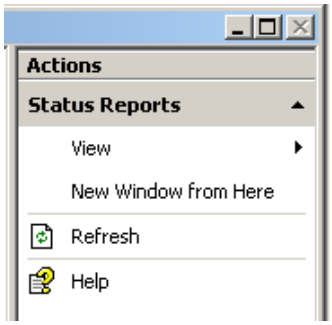


Windows MMC v3.0 includes a feature called the **Action pane**. To enable this feature, click the **Show/Hide Action Pane** icon (shown circled, below), or select **View > Customize > Action pane > OK**.



The Action pane lists the actions that are available to the users, based on the currently selected items in the tree on the left-hand side of the console window, or in the results pane in the center.

When enabled, the Action pane displays on the right-hand side of the MMC snap-in (shown below), and can be hidden from view by clicking the **Show/Hide Action Pane** icon again, or by deselecting the **Action pane** option in the **View > Customize** dialog box.



Note that the **Refresh** option in the Action pane does not function when a specific ProtectDrive *Status* or *User* report is selected. To refresh a report and view changes you've made to it, you must close and reopen PDMC.

© SafeNet, Inc.

Status Reports

The following *Status* reports are currently available:

- **Administration Status**—This report shows who has read or write access to ProtectDrive configuration data.
- **Configuration Status**—This report shows if there are pending updates that need processing, and which computers are managed by a configuration object.
- **Encryption Status**—This report shows which clients are fully or partially encrypted/decrypted, and which are not encrypted in the enterprise.
- **Recovery Status**—This report shows the presence of disaster recovery files for particular clients.
- **Update Status**—This report shows which clients have up-to-date settings, their last update status and time, etc.

User Reports

The following *User* reports are currently available.

- **User List Members**—This report shows which users belong to each member group.
- **Client Users**—This report shows which users can log on to a particular client.

Run the Reports

1. Make sure the **ProtectDrive Administrative Management Tools** are installed.
2. Launch the **ProtectDrive Management Console**.
3. Open the **ProtectDrive Reports** snap-in.
4. Navigate to the report to run.

Deploying Client-Side Components

ProtectDrive Client-Side components are used for management and encryption of ProtectDrive stand-alone and/or networked systems (members of a Windows Domain).

When deploying ProtectDrive Client-Side components on systems containing multiple hard disks, **disk0** must be the drive where ProtectDrive is installed.

Custom Graphics File

In addition to the installation files (shown in the example below), a custom graphics file (named **ACSGIF** or **hiresgif**, for example) may also be placed in the *\Install* directory.

This graphics file, created by SafeNet, includes the customer-specific artwork that will appear as part of the various ProtectDrive pre-boot authentication and/or system recovery display screens. If this file is present, the ProtectDrive installer will automatically include this file as part of the Client-Side Component installation.

Install the ProtectDrive Client-Side Components

If you are deploying ProtectDrive on a Windows 7, Windows Vista, or Windows Server 2008 client, run **Setup.exe** (located in the same directory) instead of **SafeNet ProtectDrive.msi**.

Name	Size	Type	Date Modified
1031.mst (German)	103 KB	MST File	1/5/2011 5:41 PM
1033.mst (English)	4 KB	MST File	1/5/2011 5:41 PM
1041.mst (Japanese)	98 KB	MST File	1/5/2011 5:41 PM
SafeNet ProtectDrive.msi	23,317 KB	Windows Installer Package	1/5/2011 5:42 PM
Setup.exe	56 KB	Application	1/5/2011 5:39 PM

© SafeNet, Inc.

Changing the Default Language

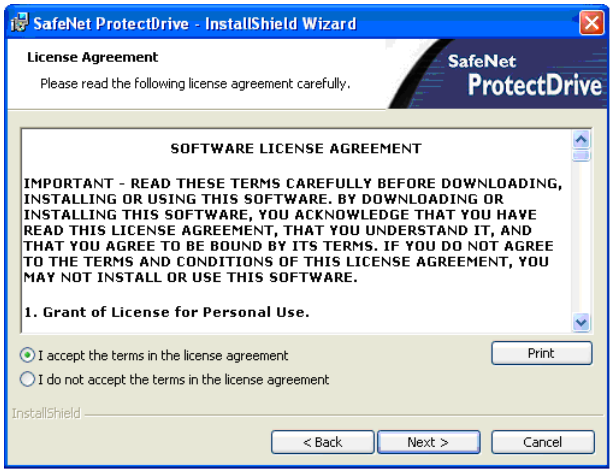
The default language for the ProtectDrive installation wizard is English. Use a different MST file (shown in the example above) to change the language. As an example, to change the ProtectDrive installation to Japanese, go to the DOS prompt and type the following command line:

```
msiexec.exe /i "SafeNet ProtectDrive.msi" TRANSFORMS=1041.mst
```

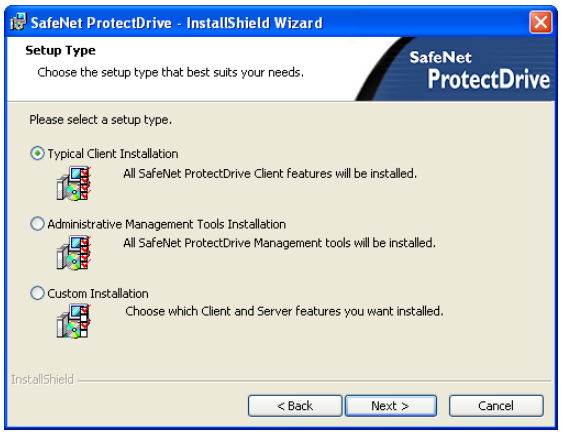
1. Launch the **SafeNet ProtectDrive.msi.** The ProtectDrive installation wizard opens.
2. When the **Welcome** screen displays, click **Next**.

SafeNet ProtectDrive - InstallShield Wizard
Welcome to the InstallShield Wizard for SafeNet ProtectDrive
The InstallShield(R) Wizard will install SafeNet ProtectDrive on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
SafeNet ProtectDrive
< Back
Next >
Cancel

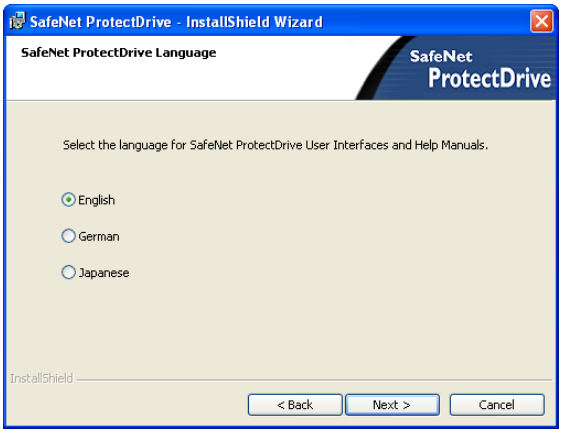
3. Read and accept the **License Agreement**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SafeNet ProtectDrive
SOFTWARE LICENSE AGREEMENT
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.
1. Grant of License for Personal Use.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

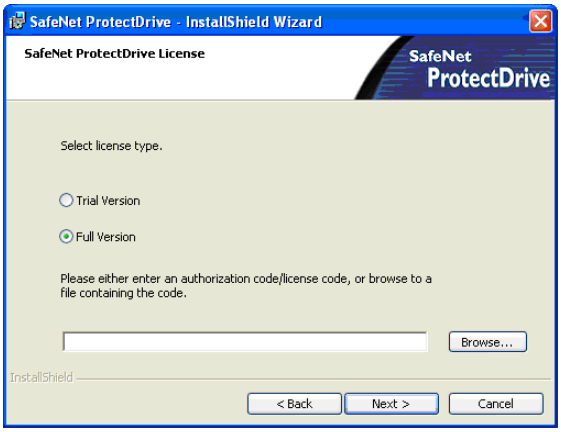
4. Select **Typical Client Installation**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
SafeNet ProtectDrive
Please select a setup type.
Typical Client Installation
All SafeNet ProtectDrive Client features will be installed.
Administrative Management Tools Installation
All SafeNet ProtectDrive Management tools will be installed.
Custom Installation
Choose which Client and Server features you want installed.
InstallShield
< Back
Next >
Cancel

5. Select the language to be used for interface labels and text messages, and then click **Next**.



6. Select the license type, and then click **Next**.



© SafeNet, Inc.

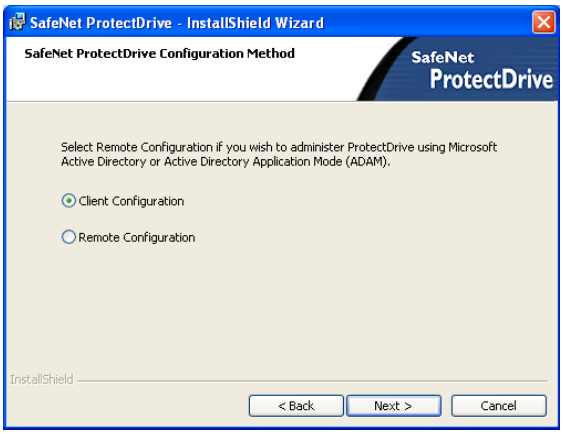
- If you select **Trial Version**, a 30-day evaluation version of ProtectDrive will be installed. (After installation, a trial license can be updated to a valid, full license via the LMC **License Manager** tab.)

- If you select **Full Version**, you must have either a valid license code (for example, **license.txt**) or authorization code (for example, **authorization.txt**). The default path for the license/authorization file is the source directory (from which the **SafeNet ProtectDrive.msi** file is run).

  - To enter the license code or authorization code, either browse to and open the file, copy and paste the entire contents into the browse field, and then click **Next**, or browse to the license file and click **Next**.

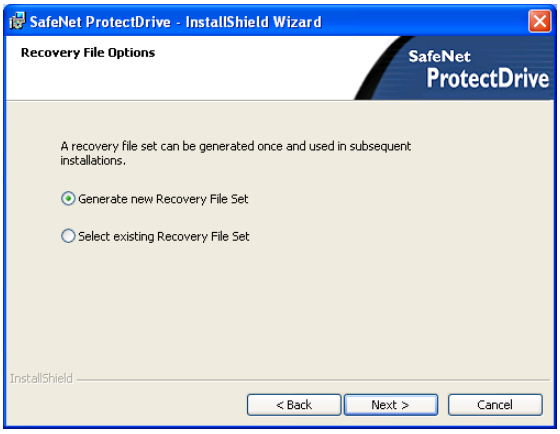
  - To enter the authorization code, an Internet connection is necessary to contact the license server. Browse to the authorization file, and then click **Next**. The license server is contacted (via the Internet connection), and will, in turn, provide an authorization code to allow the installation to continue.

7. Choose the appropriate ProtectDrive configuration method. Select **Client Configuration** for stand-alone installations, or select **Remote Configuration** for remote configuration using Active Directory/ADAM, and then click **Next**. If you select **Remote Configuration**, you **must** have an existing recovery file set to use in step 9.

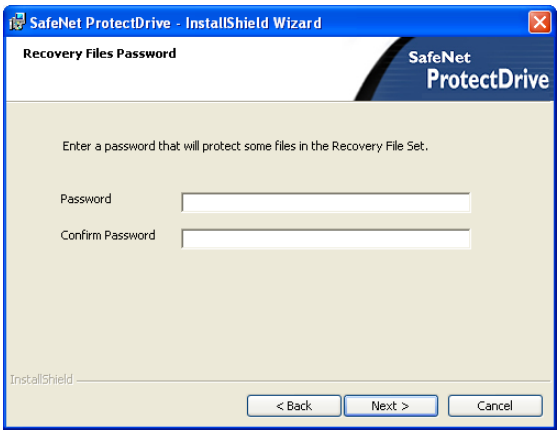

SafeNet ProtectDrive - InstallShield Wizard
SafeNet ProtectDrive Configuration Method
SafeNet
ProtectDrive
Select Remote Configuration if you wish to administer ProtectDrive using Microsoft Active Directory or Active Directory Application Mode (ADAM).
Client Configuration
Remote Configuration
InstallShield
< Back
Next >
Cancel

If you select the **Client Configuration** method, then the **Advanced > Management** update options in the **Local Management Console** will be unavailable because those options only apply to Active Directory/ADAM.

8. Choose the appropriate recovery file set option, and then click **Next**.



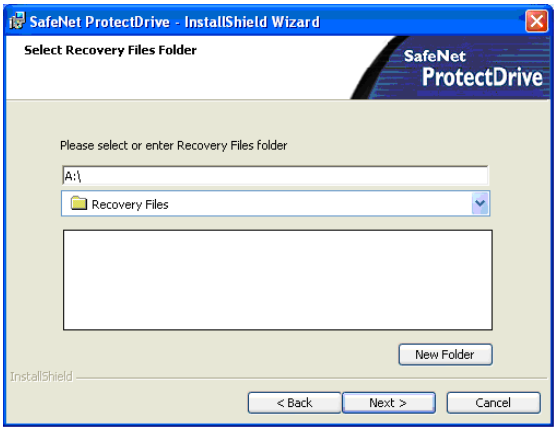
- If you select the **Select existing Recovery File Set** option, skip to step 10.
- If you select the **Generate new Recovery File Set** option, the following screen displays. Enter and confirm the recovery file set password, and then click **Next**.



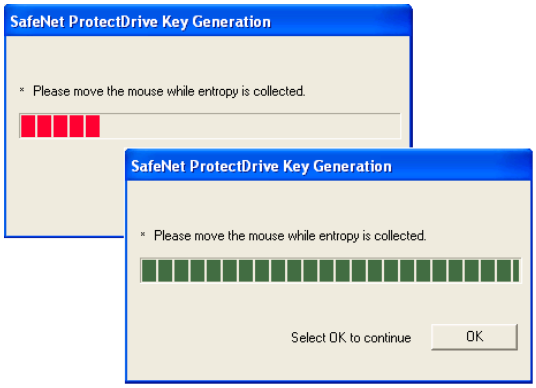
9. Select the recovery files folder location, and then click **Next**.
   - If you chose the **Select existing Recovery File Set** option in step 8, the recovery files folder is the location where the existing files are located.

© SafeNet, Inc.

- If you chose the **Generate new Recovery File Set** option in step 8, the recovery files folder is the location where the new recovery file set you are creating will be stored. Choose a secure location, on your network, a floppy drive, or any other location **except** the local drive.



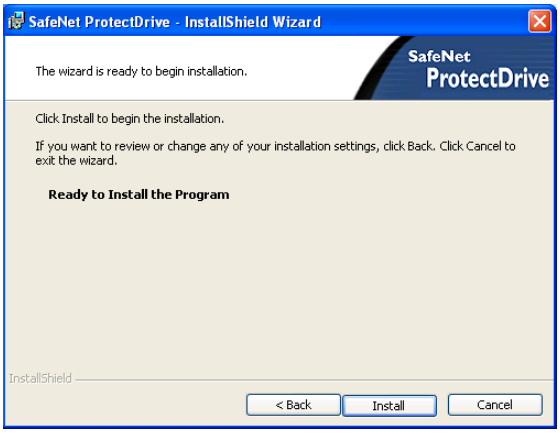
10. The system will proceed to collect entropy to generate the recovery files. Move the mouse, and then click **OK** when it is completed.


SafeNet ProtectDrive Key Generation
* Please move the mouse while entropy is collected.
SafeNet ProtectDrive Key Generation
* Please move the mouse while entropy is collected.
Select OK to continue
OK

11. A prompt, similar to the one shown below, will display if the recovery files were successfully created. Click **OK** to continue.

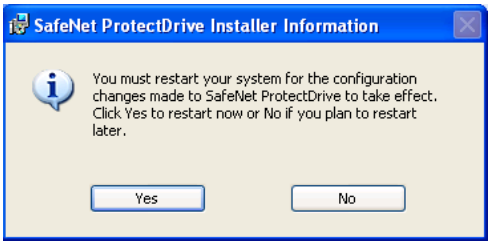
SafeNet ProtectDrive - InstallShield Wizard
Label and store safely the SafeNet ProtectDrive key files in A:\ after the installation is complete.
OK

12. When the following screen displays, click **Install** to begin the installation.


SafeNet ProtectDrive - InstallShield Wizard
The wizard is ready to begin installation.
SafeNet
ProtectDrive
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Ready to Install the Program
InstallShield
< Back
Install
Cancel

13. When the following screen displays, click **Finish**.

14. When prompted, click **Yes** to restart the PC.


SafeNet ProtectDrive Installer Information
You must restart your system for the configuration changes made to SafeNet ProtectDrive to take effect. Click Yes to restart now or No if you plan to restart later.
Yes
No

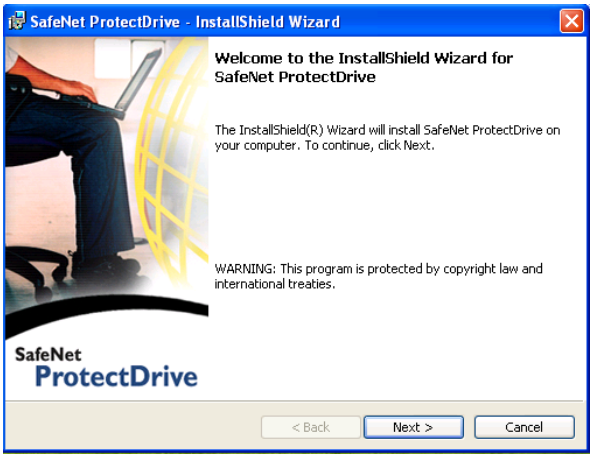
© SafeNet, Inc.

Customizing the Installation

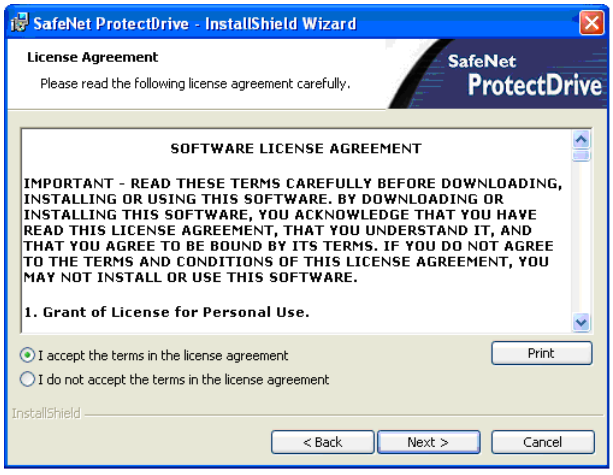
In addition to Server and Client component installations, ProtectDrive provides the ability to custom-select the install components.

If you are deploying ProtectDrive on a Windows 7, Windows Vista, or Windows Server 2008 client, run **Setup.exe** (located in the same directory) instead of **SafeNet ProtectDrive.msi**.

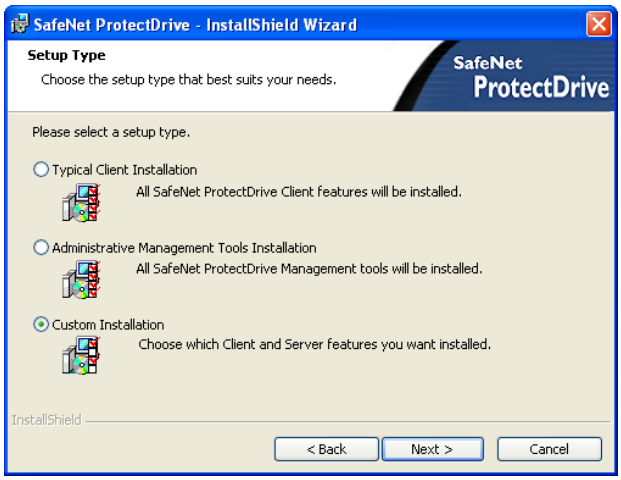
1. Launch the **SafeNet ProtectDrive.msi**. The ProtectDrive installation wizard opens.
2. When the **Welcome** screen displays, click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
Welcome to the InstallShield Wizard for SafeNet ProtectDrive
The InstallShield(R) Wizard will install SafeNet ProtectDrive on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
SafeNet
ProtectDrive
< Back
Next >
Cancel

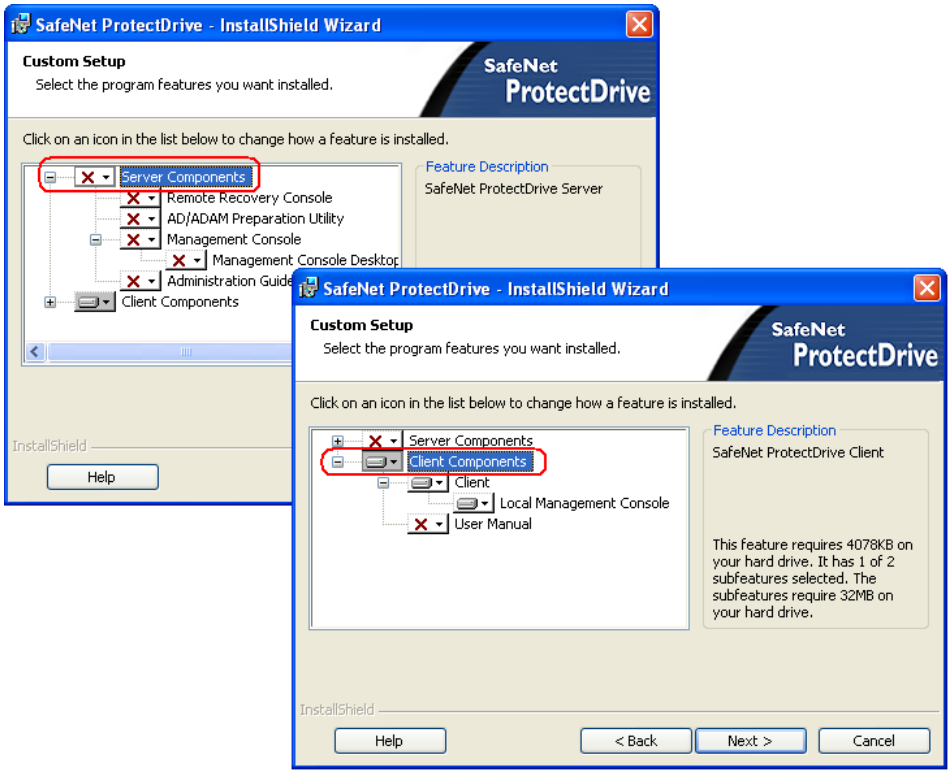
3. Read and accept the **License Agreement**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SafeNet
ProtectDrive
SOFTWARE LICENSE AGREEMENT
IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.
1. Grant of License for Personal Use.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel

4. Select **Custom Installation**, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
Setup Type
Choose the setup type that best suits your needs.
SafeNet ProtectDrive
Please select a setup type.
Typical Client Installation
All SafeNet ProtectDrive Client features will be installed.
Administrative Management Tools Installation
All SafeNet ProtectDrive Management tools will be installed.
Custom Installation
Choose which Client and Server features you want installed.
InstallShield
< Back
Next >
Cancel

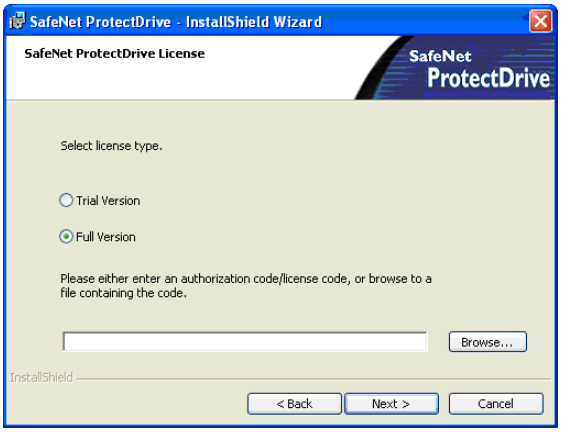
5. Select the **Server Components** and/or **Client Components** that you wish to install, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
Custom Setup
Select the program features you want installed.
SafeNet ProtectDrive
Click on an icon in the list below to change how a feature is installed.
Server Components
Remote Recovery Console
AD/ADAM Preparation Utility
Management Console
Management Console Desktop
Administration Guide
Client Components
Feature Description
SafeNet ProtectDrive Server
InstallShield
Help
SafeNet ProtectDrive - InstallShield Wizard
Custom Setup
Select the program features you want installed.
SafeNet ProtectDrive
Click on an icon in the list below to change how a feature is installed.
Server Components
Client Components
Client
Local Management Console
User Manual
Feature Description
SafeNet ProtectDrive Client
This feature requires 4078KB on your hard drive. It has 1 of 2 subfeatures selected. The subfeatures require 32MB on your hard drive.
InstallShield
Help
< Back
Next >
Cancel

© SafeNet, Inc.

Server Components	
Remote Recovery Console	This selection installs **rpadmin.exe** (the Remote Recovery Console). Refer to *Chapter 10 - Extraordinary Authentication Scenarios* for additional information.
AD/ADAM Preparation Utility	This selection installs the ProtectDrive Preparation Utility for ADAM/Active Directory Schema Extensions. Refer to page 55 for details on this utility.
Management Console	This selection installs the **Management Console**, which includes the **Active Directory Users and Computers** MMC, **ProtectDrive Management**, and **ProtectDrive Reports** snap-ins. These snap-ins are required to manage the ProtectDrive System and User policy from the server, and view various status reports, such as the **Update Status** report (shows which clients have up-to-date settings and the last time they were updated), and the **Encryption Status** report (shows which clients are not encrypted, which are, and with what). The sub-feature **Management Console Desktop** selection adds a shortcut named **ProtectDrive Management Console** to the Windows desktop.
Administration Guide	This selection installs the *SafeNet ProtectDrive Administration Guide*.
Client Components	
Local Management Console	This selection installs the Local Management Console (LMC) application, which is used to manage or view the ProtectDrive clients locally.
User Manual	This selection installs the *SafeNet ProtectDrive User Manual*.

6. Select the license type, and then click **Next**.



- If you select **Trial Version**, a 30-day evaluation version of ProtectDrive will be installed. (After installation, a trial license can be updated to a valid, full license via the LMC **License Manager** tab.)

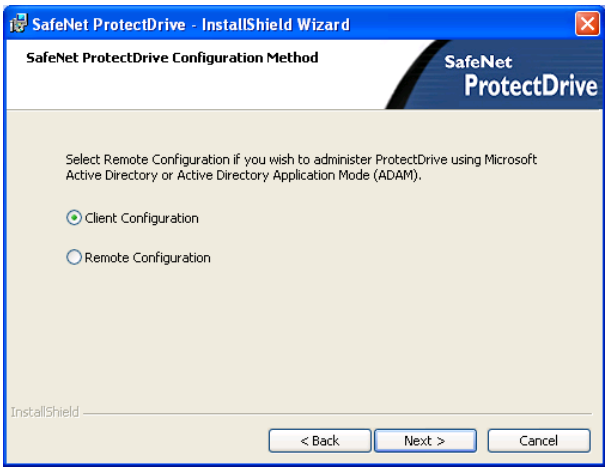
- If you select **Full Version**, you must have either a valid license code (for example, **license.txt**) or authorization code (for example, **authorization.txt**). The default path for the license/authorization file is the source directory (from which the **SafeNet ProtectDrive.msi** file is run).

  - To enter the license code or authorization code, either browse to and open the file, copy and paste the entire contents into the browse field, and then click **Next**, or browse to the license file, and then click **Next**.

  - To enter the authorization code, an Internet connection is necessary to contact the license server. Browse to the authorization file, and then click **Next**. The license server is contacted (via the Internet connection), and will, in turn, provide an authorization code to allow the installation to continue.

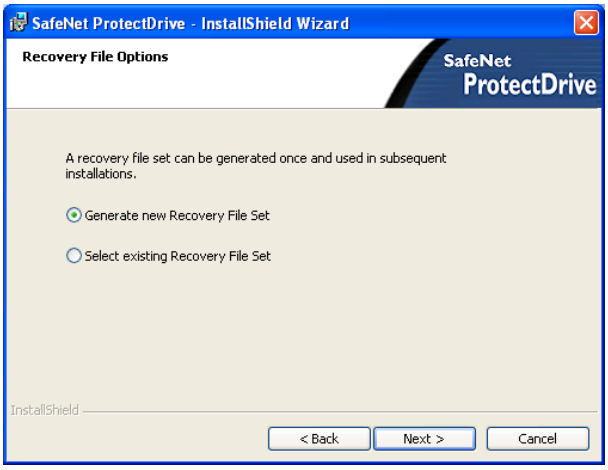
© SafeNet, Inc.

7. Choose the appropriate ProtectDrive configuration method. Select **Client Configuration** for stand-alone installations, or select **Remote Configuration** for remote configuration using Active Directory/ADAM, and then click **Next**.


SafeNet ProtectDrive - InstallShield Wizard
SafeNet ProtectDrive Configuration Method
SafeNet ProtectDrive
Select Remote Configuration if you wish to administer ProtectDrive using Microsoft Active Directory or Active Directory Application Mode (ADAM).
Client Configuration
Remote Configuration
InstallShield
< Back
Next >
Cancel

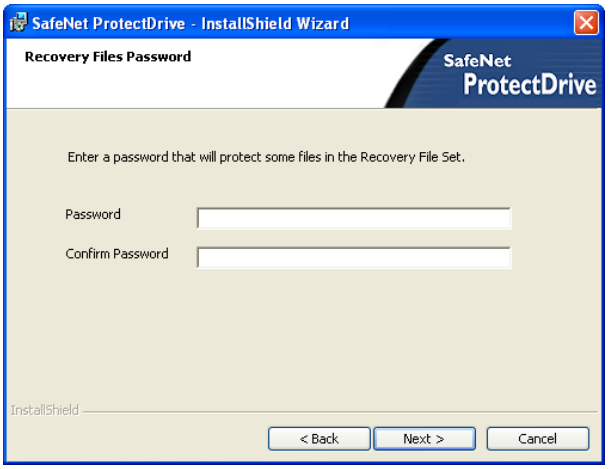
If you select the **Client Configuration** method, then the **Advanced > Management** update options in the **Local Management Console** will be unavailable because those options only apply to Active Directory/ADAM.

8. Choose the appropriate recovery file set option, and then click **Next**.

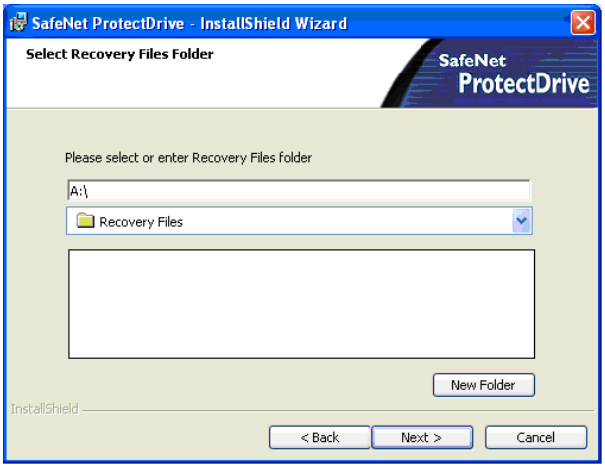

SafeNet ProtectDrive - InstallShield Wizard
Recovery File Options
SafeNet ProtectDrive
A recovery file set can be generated once and used in subsequent installations.
Generate new Recovery File Set
Select existing Recovery File Set
InstallShield
< Back
Next >
Cancel

If the client installation is to be remotely configured (as determined in step 7), then the Recovery File Set must have already been generated by either a previous installation or via the **Certificate Wizard** utility (refer to page 24).

- If you select the **Select existing Recovery File Set** option, skip to step 10.
- If you select the **Generate new Recovery File Set** option, the following screen displays. Enter and confirm the recovery file set password, and then click **Next**.

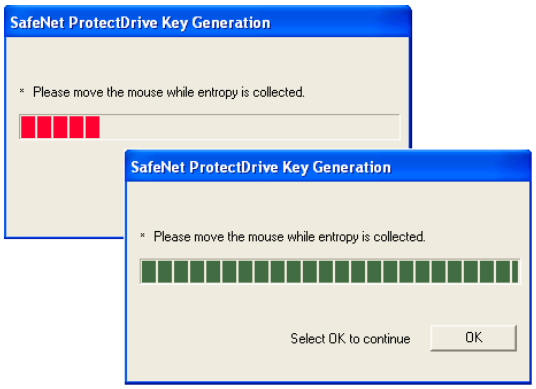


9. Select the **Recovery Files folder** location, and then click **Next**.
   - If you chose the **Select existing Recovery File Set** option in step 8, the Recovery Files folder is the location where the existing files are located.
   - If you chose the **Generate new Recovery File Set** option in step 8, the Recovery Files folder is the location where the new recovery file set you are creating will be stored. Choose a secure location, on your network, a floppy drive, or any other location **except** the local drive.



© SafeNet, Inc.

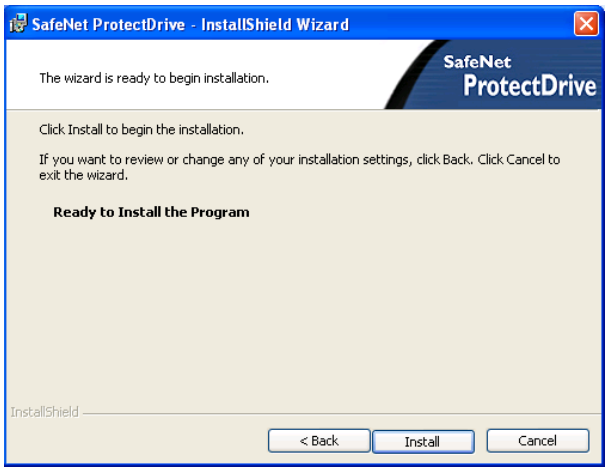
10. The system will proceed to collect entropy to generate the recovery files. Move the mouse, and then click **OK** when it is completed.


SafeNet ProtectDrive Key Generation
* Please move the mouse while entropy is collected.
SafeNet ProtectDrive Key Generation
* Please move the mouse while entropy is collected.
Select OK to continue
OK

11. A prompt, similar to the one shown below, will display if the recovery files were successfully created. Click **OK** to continue.

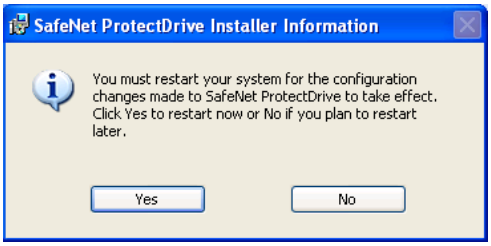
SafeNet ProtectDrive - InstallShield Wizard
Label and store safely the SafeNet ProtectDrive key files in A:\ after the installation is complete.
OK

12. When the following screen displays, click **Install** to begin the installation.


SafeNet ProtectDrive - InstallShield Wizard
The wizard is ready to begin installation.
SafeNet ProtectDrive
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Ready to Install the Program
InstallShield
< Back
Install
Cancel

13. When the following screen displays, click **Finish**.

14. When prompted, click **Yes** to restart the PC.


SafeNet ProtectDrive Installer Information
You must restart your system for the configuration changes made to SafeNet ProtectDrive to take effect. Click Yes to restart now or No if you plan to restart later.
Yes
No

© SafeNet, Inc.

Disk Imaging—Norton™ Ghost™ Interoperability with ProtectDrive (version 9.0 and higher)

Disk imaging is a way to replicate the complete contents and structure of a hard drive or other data storage device. This method—also called ―ghosting"—can be used to clone a fully-prepared ProtectDrive system, which can then be rapidly deployed to a large number of computers in an enterprise.

An installation of ProtectDrive is designed to modify the Master Boot Record (MBR) and encrypt the entire drive/partition. Attempting to back up such a drive, using a program such as Norton Ghost™, can result in some confusion. There is an option in Ghost to back up the MBR and the entire disk contents (including free space). However, this is incompatible with ProtectDrive.

Imaging a ProtectDrive system must be done sector-by-sector to create a compatible backup. Ghost offers an option called *RAW* mode to preserve sectors. This document describes how to use Ghost in RAW mode to create a backup of an encrypted system.

Using Norton Ghost™ in RAW Mode

Command line options (switches) can be specified when running the Norton Ghost program. Note that not all switches are available in all versions.

To launch Ghost in *RAW* mode, run the DOS mode *Ghost.exe* file (distributed with Norton Ghost) with the ―image raw" command line switch, *-ir*. The *–ir* switch is available in Norton Ghost 2002 and later.

When *–ir* is used, disk backup operations will be performed in RAW mode, and an *"Image RAW"* message will display while Ghost is in progress. The *–ir* switch tells Ghost to create a sector-by-sector copy without attempting to repair minor boot track problems. The result is an image file that is an exact duplicate of the source disk, which includes extraneous or erroneous boot track information.

Partitions are not resized when Ghost is performing sector copies. For more information on this and the other sector-copy switches, refer to the following Symantec™ documents:

- ―*Forensic imaging using Ghost*," at: http://entsupport.symantec.com/docs/n1999110813413225.
- ―*Switches: Sector copy*" at: http://service1.symantec.com/SUPPORT/on-technology.nsf/docid/2001111413481325.

Creating a Unique Disk Key for Each Deployed System

If you image a ProtectDrive system which has pre-boot activated, all systems that are deployed with that image will have the same disk encryption key. Currently, there is no mechanism in ProtectDrive to change a disk key after installation, other than to deactivate pre-boot, and then re-activate it, which involves a full decryption and re-encryption. This is a time-consuming and undesirable scenario.

It is highly recommend that each system has a unique disk encryption key. But how do you deploy a ProtectDrive image onto many computers, while ensuring the disk keys are unique for each system? At what point should an image be created to ensure this occurs?

To ensure unique disk keys, create the initial system image after ProtectDrive is installed, but before the first boot is performed (immediately after installation is complete). In this state, the imaged system will not have pre-boot activated, and therefore, would not yet have a disk key. Later, when this image is deployed, and as each system is booted up, pre-boot is activated, and if so configured, will start the encryption.

Follow this procedure to create a unique key for each computer:

1. Install ProtectDrive on the computer to be imaged.
2. When the installation is complete, shut down the computer.
3. Image the hard drive using Norton Ghost.
4. Distribute the image on a computer.
5. Boot the computer and activate pre-boot. A unique disk encryption key is generated at this point for this computer.
6. Repeat steps 4 and 5 on all computers.

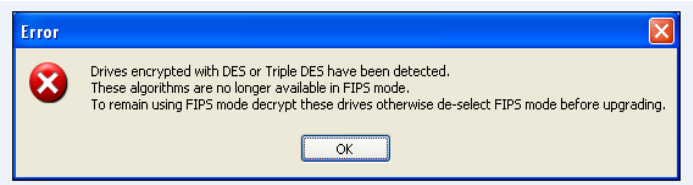
When distributing a ghosted ProtectDrive image, it must be put back on a drive with the same geometry as the original ghosted system.

© SafeNet, Inc.

Upgrading From a Previous Version of ProtectDrive

Before You Begin

- The latest version of ProtectDrive supports upgrades from versions 8.2.1, 8.3.0, 8.4.x, 8.5.x, 9.0.x, 9.1.x, 9.2.x, 9.3.x, and 9.4.x.
- Prior to upgrading a system that is FIPS-enabled and has DES or Triple DES-encrypted drives, you must either decrypt the drives or disable FIPS mode. Otherwise, the upgrade will fail and the following message will display:


Error
Drives encrypted with DES or Triple DES have been detected.
These algorithms are no longer available in FIPS mode.
To remain using FIPS mode decrypt these drives otherwise de-select FIPS mode before upgrading.
OK

- Re-run **PDDirPrep** when you are upgrading Active Directory or ADAM to a new version of ProtectDrive.
- When upgrading a server and remote clients, always upgrade the server first.
- After upgrading from ProtectDrive version 8.2.1 (or higher) to the latest version, all existing clients will be recognized as managed by the property sheet of their own computer objects. They will function no differently than they did before the upgrade. Once the clients are upgraded to the latest version, they can be configured to retrieve their policy from any Configuration Object. (After the upgrade, change their policy configuration assignment from **Managed by this property sheet** to **Managed by a configuration object**. Refer to page 59 for details.)
- If you currently have ProtectDrive installed on a Windows XP or Windows 7 client, and you intend to upgrade to a Windows Vista client, **and** upgrade to ProtectDrive version 8.3 (or higher), you must uninstall the current version of ProtectDrive, upgrade to Windows Vista, and then run a clean (new) installation of ProtectDrive.
- If you are currently using Active Directory, you should continue to use it when you upgrade rather than changing to ADAM, as there is no real benefit to the change.

  However, if you do choose to change from Active Directory to ADAM, you must:

  - Remove ProtectDrive on the server (refer to page 84).
  - Install the **Administrative Management Tools**.
  - Create an ADAM instance (on a separate machine, not the domain controller) by using the **PDDirPrep** utility).

    Please be aware that after changing from Active Directory to ADAM, you will have two sets of schema extensions. Even though ProtectDrive is uninstalled and reinstalled, the schema extensions cannot be removed from the Active Directory server.

Creating a New Recovery File Set

A recovery file set should include these files for an upgrade: *PdMaster.cer/.pfx*, *PdRecovery.cer/.pfx*, *salt.cid*, and *<computername>_license.txt*. There are two ways to create the **PdMaster** and **PdRecovery** files:

- Generate them during a new ProtectDrive installation. (A backup of the license file will also be created at the same time.)
- Create them using the **Certificate Wizard** (**certwizardapp.exe**). Refer to page 24 for details on how to use this utility.

Do **not** create a new salt.cid key in the **Certificate Wizard** to upgrade a client.

Any time the license changes, it is good practice to run the backup.exe utility to ensure your recovery file set is up-to-date. Refer to Chapter 11 for details on the backup utility.

About Interactive Upgrades

You can choose to either generate a new recovery file set or use an existing ProtectDrive version 8.2.1 (or higher) file set.

- If you choose to generate a new file set, the PdMaster and PdRecovery files and a backup of the license file will be created during the install.
- If you choose to use an existing file set, the PdMaster and PdRecovery files must be previously created from a previous install, or from **Certificate Wizard**.
- If you are upgrading multiple clients, it is recommended that you use an existing file set.
- If you are upgrading a server and remote clients, upgrade the server first.

About Silent/GPO Upgrades

This requires that you use an existing recovery file set. The recovery file set should be located in the same directory as the **SafeNet ProtectDrive.msi** file, or it should be in the path defined by the **ERA_KM_REC_FILE_FOLDER_PATH** MSI property.

The directory specified here must be **writeable**, since the *RecoveryEnvelope.env* file (and the *<computername>_license.txt* file) will be created in this directory. If Active Directory or ADAM is being used, the *RecoveryEnvelope.env* file will also be copied to the management server.

© SafeNet, Inc.

Upgrade Procedure

A ProtectDrive upgrade is initiated the same way as a new client installation—run the **SafeNet ProtectDrive.msi**. The system will detect that an earlier version of ProtectDrive is installed.

When upgrading the server, you will be prompted to select an MSO certificate that must have a signed value. This certificate ensures that a server or client will connect to an ADAM instance that has a Service Connection Point (SCP) with a signed MSO value.

The upgrade installation screens are basically the same as a new installation.

Refer to page 64 for step-by-step installation details.

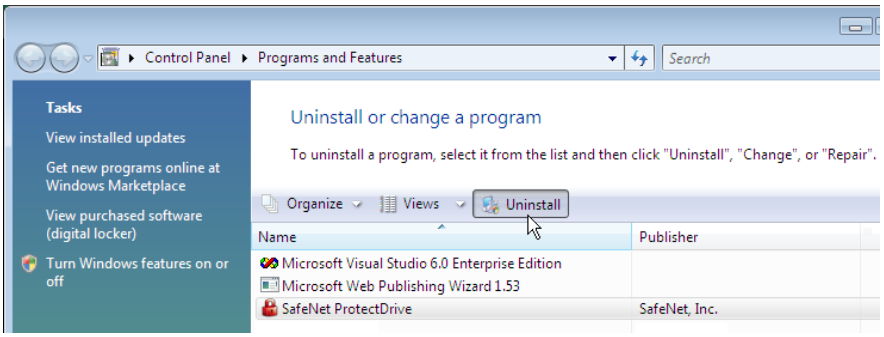
As a reminder, prior to upgrading a system that is FIPS-enabled and has DES or Triple DES-encrypted drives, you must either decrypt the drives or disable FIPS mode. Otherwise, the upgrade will fail.

Uninstalling ProtectDrive

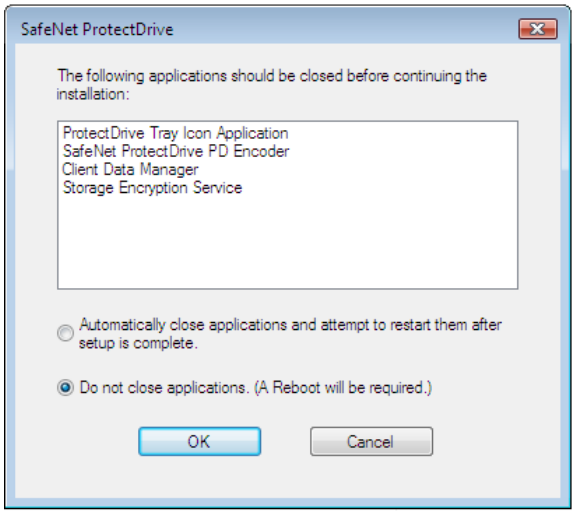
Windows Vista

Follow this procedure to uninstall ProtectDrive from a Windows Vista system.

1. Make sure that all partitions are decrypted.
2. Navigate to **Programs and Features** in the Windows Control Panel.
3. Select **SafeNet ProtectDrive**, and then click **Uninstall**.



4. When prompted, click **Yes** to confirm the action.
5. A list of currently open applications displays. Click the **Do not close the applications** option, and then click **OK**.


SafeNet ProtectDrive
The following applications should be closed before continuing the installation:
ProtectDrive Tray Icon Application
SafeNet ProtectDrive PD Encoder
Client Data Manager
Storage Encryption Service
Automatically close applications and attempt to restart them after setup is complete.
Do not close applications. (A Reboot will be required.)
OK
Cancel

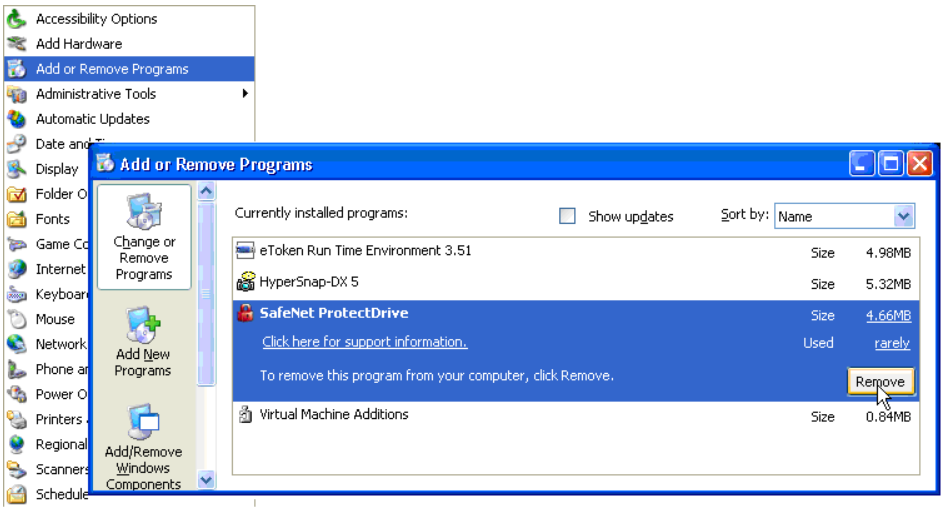
6. When prompted, click **Yes** to restart the computer.

© SafeNet, Inc.

Windows 2003, 2008, or XP

Follow this procedure to uninstall ProtectDrive from a Windows 2003, 2008, or XP system.

1. Make sure that all partitions are decrypted.
2. Navigate to **Add or Remove Programs** in the Windows Control Panel.
3. Select **SafeNet ProtectDrive**, and then click **Remove**.

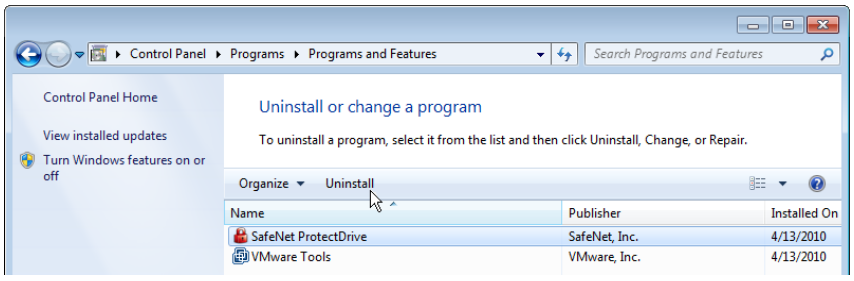


4. When prompted, click **Yes** to confirm the action.
5. When prompted, click **Yes** to restart the computer.

Windows 7

Follow this procedure to uninstall ProtectDrive from a Windows 7 system.

1. Make sure that all partitions are decrypted.
2. Navigate to **Programs > Programs and Features** in the Windows Control Panel.
3. Select **SafeNet ProtectDrive**, and then click **Uninstall**.



4. When prompted, click **Yes** to confirm the action.
5. When prompted, click **Yes** to restart the computer.

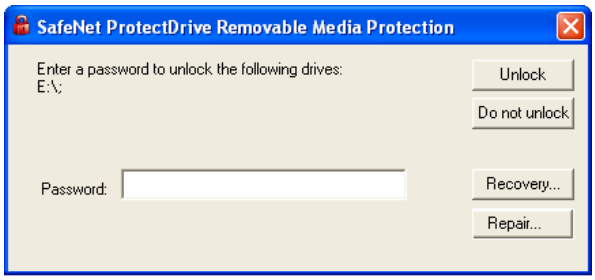
Removable Media Recovery

To ensure the recovery and reusability of a removable media device should it become unstable or compromised, follow one of these this repair procedures to remove encryption from the device and then reformat it for reuse.

Standard Recovery Procedure

This procedure should be performed for each USB flash drive that is deployed.

1. Connect the removable media to the PC. The following screen should display when the device is detected.



2. Click **Repair**.

3. Click **OK** when the following message displays:

SafeNet ProtectDrive Removable Media Protection
The encrypted status can be removed so that the drive can be formatted and usable. This will result in data loss!
Would you like SafeNet ProtectDrive to remove the encrypted status of the drive?
Yes
No

4. Click **Yes**.

5. When prompted, click **OK** and safely remove the device.

SafeNet ProtectDrive Removable Media Protection
Please remove drive E:\ and re-insert it. Then format the drive to make it usable.
OK

6. Re-connect the removable media device and reformat it for reuse. Reformatting should be done before the device is re-encrypted.

© SafeNet, Inc.

Alternate Recovery Procedure #1 (Use RmRMBR)

In the event that the *Standard Recovery Procedur*e described on the previous page does not return the device to a reusable state, follow the steps in this section. Contact SafeNet Support prior to attempting this procedure.

This procedure should be performed for each USB flash drive that is deployed.

1. Connect the removable media device to be recovered. Perform the appropriate step based on the state of the device:

   - If the device is encrypted, a password prompt will display. Enter the password, and then click **OK** to continue.

   - If the device is not encrypted, an encryption dialog box will display. Click **Do not encrypt**.

2. Go to the command line. To do so:

   - From the Windows desktop, select **Start > Run**.

   - In the **Run** dialog box, enter **cmd**, and then click **OK**.

3. Change to the ProtectDrive directory:

   cd \Program Files\SafeNet ProtectDrive

4. Run the recovery utility:

   rmrmbr /d *x*:

   (where ***x*** equals the drive letter of the removable media device)

5. A prompt displays stating that you are about to remove ProtectDrive from the device. Press **Enter** to confirm and continue. (If you wish to abort, press **Ctrl+C**.)

6. When prompted, safely remove the removable media device.

7. Re-connect the removable media device and reformat it for reuse.

If this procedure does not fully recover the device, perform the procedures outlined in the next section.

Alternate Recovery Procedure #2 (Use Sector 0 Backup Data)

In the event that the *Standard Recovery Procedur*e and the first alternate recovery procedure (using RmRMBR) described on the previous pages does not return the device to a reusable state, follow the steps in this section. Contact SafeNet Support prior to attempting this procedure.

You must already have a backup of the device's Sector 0 data (from the backup created on page 23) in order to restore the device using the procedure outlined below.

The steps in this section will restore the Sector 0 data to the USB flash drive, which will allow the device to be reformatted for reuse. This procedure should be performed **on each USB flash drive that is deployed**.

1. Insert the USB flash drive into a computer that does not have ProtectDrive installed.
2. Run the **dskprobe** utility. (This utility is included in the Microsoft Windows 2003 Resource Kit and can be downloaded from the Internet.)
3. Select **File > Open File**. Open the file with the saved Sector 0 data for this USB flash device.
4. Select **Drives > Physical Drive**.
5. Double-click the last drive in the list, which should be the USB flash drive. It will appear under **Handle 0** in the bottom of the screen.
6. De-select the **read only** option so that you can write to the device.
7. Select **Set Active** for that drive, and then select **OK**.
8. Make no changes to the default settings. Select **Sectors > Write**, and then click **Write it**.
9. Respond **Yes** to any warnings that display.

When you attempt to access the drive, you will be prompted to format it, which you can now safely do.

© SafeNet, Inc.

Exporting the Client Configuration Settings (.XML file)

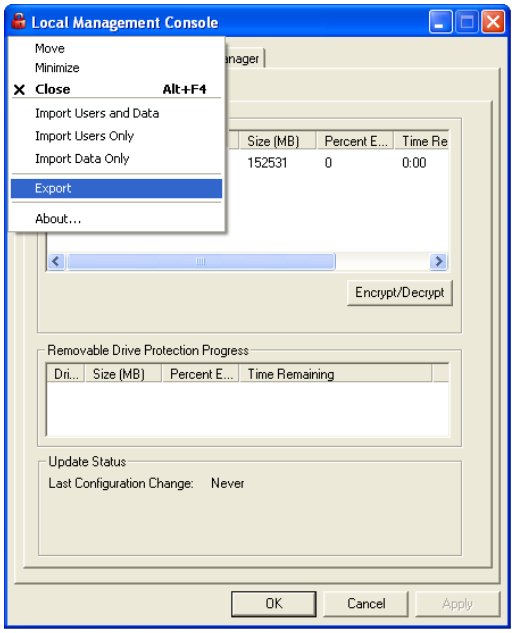
After you have installed and configured the desired ProtectDrive settings on a client PC, you can export the settings to an .XML file, and then import the file to multiple clients. This .xml file is encrypted using the salt.cid file (used for removable media recovery). Therefore, you can only import this file to client PCs that share the same salt.cid.

For large installations, multiple client PCs can be configured quickly with an exported .XML file from another ProtectDrive-configured client in your network.

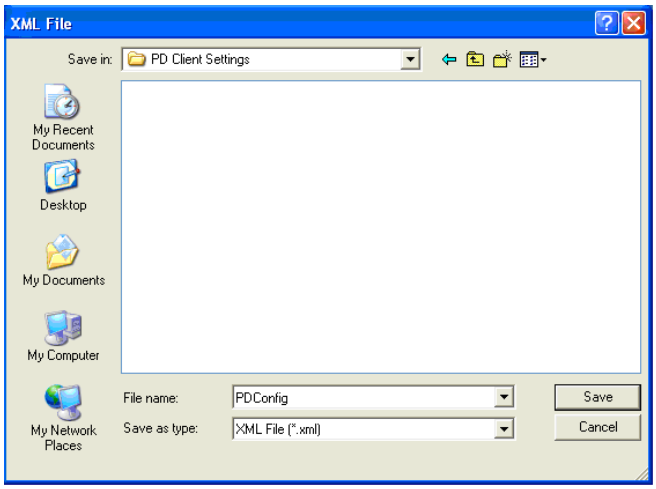
You can use this exported .xml file in a GPO installation by including the **ERA_ CONFIG_FILE_XML_PATH** property in the customized **SafeNet ProtectDrive.msi** file. Refer to page 42 for details.

Follow these steps to export the client settings to an XML file:

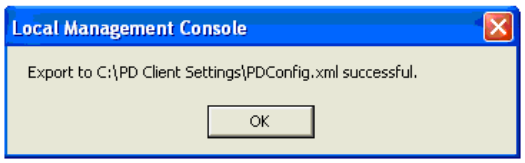
1. Open the **Local Management Console** on the configured client.
2. Click the ProtectDrive icon in the upper-left corner of the screen.
3. Select **Export**.



4. Select a location to save the .xml file, and then click **Save**. The default filename is **PDConfig.xml**.



5. Click **OK** when the file is successfully exported and saved. You can now import this file (its user or data settings, or both) to multiple clients, as needed. Refer to the next section for step-by-step instructions.



© SafeNet, Inc.

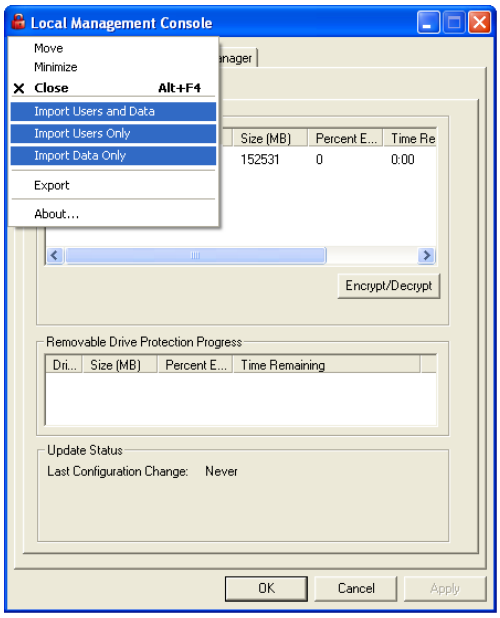
Importing the Client Configuration Settings (.XML file)

If you have saved the ProtectDrive client settings from another client PC to an .xml file, you can import the user or data settings (or both) to other client PCs that should have the same configuration. This .xml file is encrypted using the salt.cid file (used for removable media recovery). Therefore, you can only import this file to client PCs that share the same salt.cid.

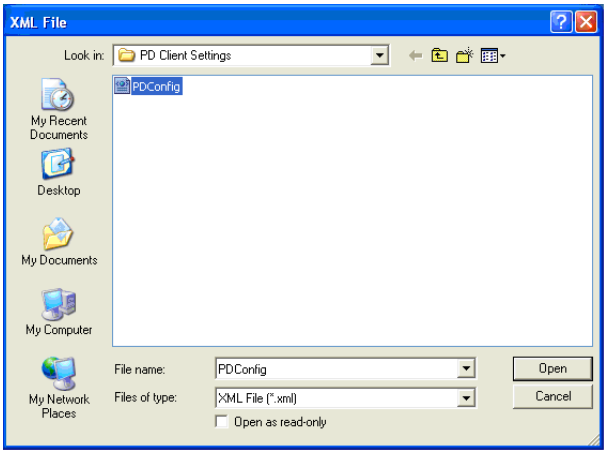
The client PCs must have ProtectDrive installed before the configuration settings can be imported.

Follow these steps to import the client settings from an XML file:

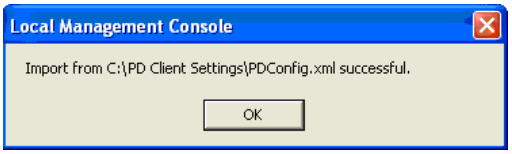
1. Open the **Local Management Console** on the client to configure.
2. Click the ProtectDrive icon in the upper-left corner of the screen.
3. Select **Import Users and Data**, **Import Users Only**, or **Import Data Only**.



4. Locate and select the .xml file to import, and click **Open**.



5. Click **OK** when the file is successfully imported to the client.



6. Repeat this procedure on as many client PCs that require the same ProtectDrive configuration settings, and use the same salt.cid.

© SafeNet, Inc.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 6
Single Sign-On Management

Introduction

This chapter is only relevant to non-Windows Vista users. If you are a Windows Vista user, no action is required for single-sign on.

This chapter is specific to the use of the **GINA** (graphical identification and authentication) library. GINA, a component of Microsoft Windows operating systems *prior to Windows Vista,* provides secure authentication and interactive logon services.

If you are a *Windows Vista user*, GINA was replaced by **Credential Providers**. Credential Providers allow for significantly increased flexibility in supporting multiple credential collection methods.

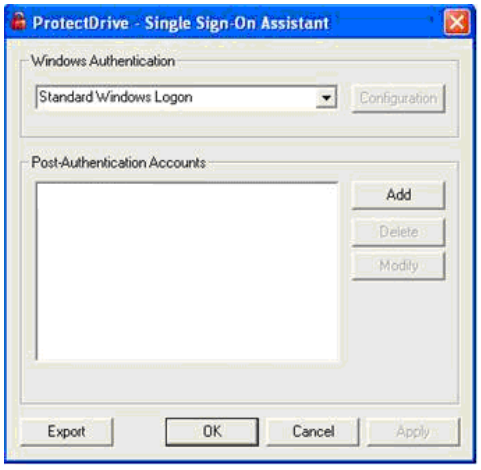
The Single Sign-On Assistant is an application that manages aspects of single sign-on for ProtectDrive. It is a flexible solution that enables users to configure the logon to their PC and other network services.

There are two components that Single Sign-On Assistant manages—Windows authentication accounts and post-authentication accounts. These components are discussed in this chapter.

Single sign-on is currently not supported with fingerprint logon.

Accessing the Single Sign-On Assistant

To access the *Single Sign-On Assistant*, execute the **ssoassistant.exe** file. This file is located in the install folder, *C:\Program Files\SafeNet ProtectDrive*.



© SafeNet, Inc.

Windows Authentication

The **Windows Authentication** field allows users to choose the GINA they would like ProtectDrive to work with. The selections are:

- **Standard Windows Logon** (msgina.dll)
- **RSA Sign-On Manager Logon** or **RSA Secure Logon** (3-gina.dll)
- **Third-party Logon**

Support for the Windows and RSA GINAs is provided with ProtectDrive (refer to the **RSA SOM Support** section, below), whereas a third-party logon must be configured by the user.

Configuration of third-party GINAs allows the selection of the GINA DLL and manual entry of the dialog and control IDs for the GINA. These settings are stored in the registry for pcvgina.dll to access during Windows startup.

Post-Authentication Accounts

Post-Authentication Accounts allow users to logon to multiple accounts that provide network services. There are specific user configurations which can benefit from using post-authentication accounts (refer to the **Third-Party Product Support** section on page 97).

You can add an unlimited number of fields to each account. Each field is configured by specifying which control in the application dialog box to fill with the required information (**Username**, **Password**, or **Domain**). The pre-boot user's account details are used to perform the logon, so the username, password, and domain name must be the same.

A command is added to each account to logon to the account. It is selected by choosing which button on the application dialog box should be clicked to perform the logon action.

RSA SOM Support

Overview

RSA Sign-On Manager (SOM) is an application that performs single sign-on across a number of enterprise applications. It is advantageous that ProtectDrive collaborates with RSA SOM. This section discusses how this can be achieved.

Implementation

RSA SOM is supported in ProtectDrive by allowing the ProtectDrive GINA (pcvgina.dll) to chain the RSA SOM GINA. This allows the RSA SOM to function correctly, while providing single sign-on for pre-boot users.

The ProtectDrive GINA loads the RSA SOM GINA dialog configuration when the Chained GINA registry value is set to the RSA SOM GINA. This can be configured by using the ProtectDrive *Single Sign-On Assistant*.

Considerations

Currently, the *Single Sign-On Assistant* and ProtectDrive GINA assume that the RSA SOM GINA is located in the standard location (*C:\Program Files\RSA Security\RSA Sign-On Manager Client\3-Gina.dll*).

If this is not the case, third-party GINA support should be used in the *Single Sign-On Assistant*, with these dialog fields configured as follows:

Tab	Field	Value
Notice	Dialog ID	100
Logon	Dialog ID Username control ID Password control ID Domain control ID	113 1000 1008 1009
Change Password	Dialog ID	800
Ctrl+Alt+Del	Dialog ID	400
Locked	Dialog ID	200
Unlock	Dialog ID Username control ID Password control ID Domain control ID	106 1000 1002 1009
Shutdown	Dialog ID	500

© SafeNet, Inc.

Third-Party Product Support

Overview

There are a number of third-party products that are often used concurrently with ProtectDrive. It can be beneficial if ProtectDrive can perform single sign-on for these products, while not requiring the direct support for each product.

This section discusses how this can be achieved in a flexible and minimal manner with ProtectDrive using the *Single Sign-On Assistant*.

Support for Third-Party GINAs

ProtectDrive GINA supports the chaining of any third-party GINA. In this case, the dialog configuration for the chained GINA is set up using the *Single Sign-On Assistant*, and is stored in the registry. ProtectDrive GINA loads this configuration at start up and performs single sign-on.

It is not guaranteed that this approach will work for every third-party GINA, as there is considerable flexibility with the implementation of replacement GINAs. Instead, single sign-on for GINAs which ―play fair" is offered.

At this stage, the user must manually enter the dialog and control IDs using *Single Sign-On Assistant*. The user must be able to source this information from the seller/manufacturer of the third-party product. Dynamic discovery, as used for post-authentication accounts, may be added in future releases.

Support for Third-Party Accounts

Logging on to third-party products can occur using a post-authentication approach. In this case, the ProtectDrive GINA and the chained GINA are used to log on to Windows. Then, each third-party product is logged on to when the Windows shell is initialized.

This is only possible if the third-party product provides a logon application. Then the *Single Sign-On Assistant* can be used to create a post-authentication account which can be run to log on to the product using the logon application.

Administrative Procedures

Configuring After ProtectDrive Installation Over an Existing System

1. Install ProtectDrive on the system.
2. Either:
   - Run the *Single Sign-On Assistant* (**ssoassistant.exe**) to configure the SSO settings.

     -OR-
   - Import an SSO configuration by running the registry file (*.reg) exported from the *Single Sign-On Assistant*.

Configuring After Installing Additional Software to the ProtectDrive System

1. Install additional software to the ProtectDrive system that installs a replacement GINA.
2. Run the *Single Sign-On Assistant*, which detects the new replacement GINA and prompts if you would like to chain the replacement GINA with the ProtectDrive GINA.
3. Either:
   - Select not to chain the GINA. You are warned of the security implications of that selection. ProtectDrive cannot provide single sign-on and cannot enforce the login method.

     -OR-
   - Select to chain the replacement GINA, so the *Single Sign-On Assistant* chains the GINA and you can set the GINA configuration.

You must run the *Single Sign-On Assistant* after the installation of any additional software.

© SafeNet, Inc.

Changing Chained GINA

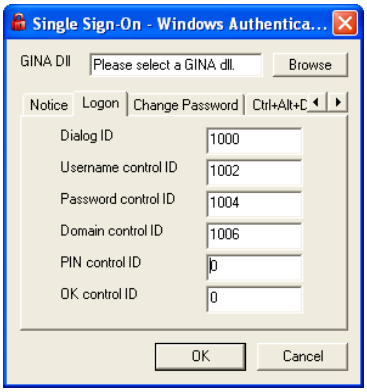
1. Run the *Single Sign-On Assistant*.
2. Select the desired GINA in the *Single Sign-On Assistant*.
3. If you select a third-party GINA, the *Single Sign-On Assistant* must be used to specify the GINA configuration.
4. Either:
   - Click **OK** or **Apply** and the Single Sign-On Assistant commits the GINA selection.

     -OR-
   - Click **Cancel** and the new GINA selection is thrown away.
5. The *Single Sign-On Assistant* exits.

Setting GINA Configuration

1. Run the *Single Sign-On Assistant*.
2. Select a third-party GINA (Standard Windows and the RSA GINAs are automatically configured).
3. Click **Configuration**.
4. Browse to the GINA DLL filename and location.
5. For each GINA dialog of interest (**Notice**, **Logon**, **Change Password**, etc.) to the ProtectDrive GINA, specify the dialog and control IDs for the third-party GINA (shown below).

   If any of the IDs are left unspecified, you will be warned that this can create unexpected behavior in the ProtectDrive GINA.



6. Either:

   - Click **OK**. The settings are stored (but not committed).

     -OR-

   - Click **Cancel**. The settings are thrown away.

7. The GINA configuration dialog closes and the main *Single Sign-On Assistant* dialog box displays.

8. Either:

   - Click **OK** or **Apply**. The settings are committed.

     -OR-

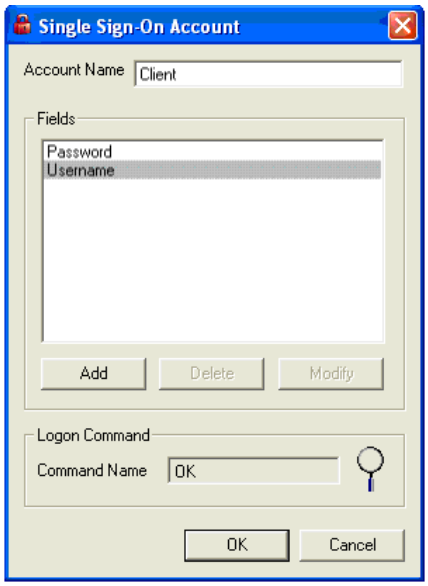
   - Click **Cancel**. The settings are thrown away.

9. The *Single Sign-On Assistant* exits.

Creating a Post-Authentication Account

1. Run the *Single Sign-On Assistant*.

2. Click **Add** to create a new account. The *Single Sign-On Account* dialog box displays.



3. Specify a unique name in the **Account Name** field.
4. Run the application. This will perform the post-authentication account logon.

© SafeNet, Inc.

5. Click **Add** in the *Single Sign-On Account* dialog box. The *Single Sign-On Field* dialog box displays.

6. Drag the magnifying glass icon/cursor from the *Single Sign-On Field* dialog box to the field required on the application logon window.

   Field Name and **Field Control** details appear in the *Single Sign-On Field* dialog box as shown in the screen shot above.

7. Choose a selection in the **Fill Field With** field, and then click **OK**.

8. Repeat steps 5 through 7 for each field you want to add.

9. Select the logon command (the button on the application which performs the logon) by dragging the magnifying glass icon/cursor from the *Single Sign-On Account* dialog box over the button on the application.

10. Either:

    - Click **OK**. The account is committed.

      -OR-

    - Click **Cancel**. The account is not created.

11. When the *Single Sign-On Account* dialog box closes, you are returned to the main *Single Sign-On Assistant* dialog box.

12. Either:

    - Click **OK** to commit the account.

      -OR-

    - Click **Cancel** to not create the account.

13. The *Single Sign-On Assistant* exits.

Modifying a Post-Authentication Account

1. Run the *Single Sign-On Assistant*.
2. Select the account to modify from the **Post Authentication Accounts** list, and then click **Modify**. The *Single Sign-On Account* dialog box displays the account information.
3. Change the account information as required.
4. Either:
   - Click **OK** to save the new account information.

     -OR-
   - Click **Cancel** to discard the account information.
5. The *Single Sign-On Account* dialog box closes and you are returned to the *Single Sign-On Assistant* dialog box.
6. Either:
   - Click **OK** to commit the new account information.

     -OR-
   - Click **Cancel** to discard the new account information.
7. The *Single Sign-On Assistant* exits.

Removing a Post-Authentication Account

1. Run the *Single Sign-On Assistant*.
2. Select the account to remove from the **Post Authentication Accounts** list, and then click **Delete**.
3. Either:
   - Select **OK** to commit the account deletion.

     -OR-
   - Select **Cancel** to not delete the account.
4. The *Single Sign-On Assistant* exits.

© SafeNet, Inc.

Creating a Post-Authentication Account Field

1. Run the *Single Sign-On Assistant*.
2. Click **Add** to create a new account, or click **Modify** to change an existing account.
3. Run the application to perform the post-authentication account logon. The *Single Sign-On Accounts* dialog box displays.
4. Click **Add**. The *Single Sign-On Field* dialog box appears.
5. Specify a unique **Account Name**.
6. Select the field control by dragging the magnifying glass icon/cursor over the control to be filled in the application.
7. Select the information to fill in the field.
8. Either:
   - Click **OK** to store the field in the account.

     -OR-
   - Click **Cancel** to discard the new field.
9. The *Single Sign-On Field* dialog box closes and user returns to the account dialog box.
10. Either:
    - Click **OK** to store the account.

      -OR-
    - Click **Cancel** to discard the new account/information.
11. The *Single Sign-On Account* dialog box closes and you are returned to the *Single Sign-On Assistant* dialog box.
12. Either:
    - Click **OK** to commit the account.

      -OR-
    - Click **Cancel** to discard the account.
13. The *Single Sign-On Assistant* exits.

Modifying a Post-Authentication Account Field

1. Run the *Single Sign-On Assistant*.
2. Click **Modify** to change an existing account.
3. Run the application to perform the post-authentication account logon. The *Single Sign-On Accounts* dialog displays.
4. Click **Modify**. The *Single Sign-On Field* dialog box displays.
5. Change the file information.
6. Either:
   - Click **OK** to store the modified field in the account.

     -OR-
   - Click **Cancel** to discard the new field information.
7. The *Single Sign-On Field* dialog box closes and you are returned to the *Single Sign-On Account* dialog box.
8. Either:
   - Click **OK** to store the account.

     -OR-
   - Click **Cancel** to discard the new field information.
9. The *Single Sign-On Account* dialog closes and you are returned to the *Single Sign-On Assistant* dialog box.
10. Either:
    - Click **OK** to commit the new field information.

      -OR-
    - Click **Cancel** to discard the account.
11. The *Single Sign-On Assistant* exits.

© SafeNet, Inc.

Removing a Post-Authentication Account Field

1. Run the *Single Sign-On Assistant*.
2. Click **Modify** to change an existing account.
3. Run the application to perform the post-authentication account logon. The *Single Sign-On Accounts* dialog box displays.
4. Click **Delete**.
5. Either:
   - Click **OK** to remove the field temporarily from the account.

     -OR-
   - Click **Cancel** to keep the field in the account.
6. The *Single Sign-On Account* dialog box closes and you are returned to the main the *Single Sign-On Assistant* dialog box.
7. Either:
   - Click **OK** to permanently delete the field from the account.

     -OR-
   - Click **Cancel** to keep the field in the account.
8. The *Single Sign-On Assistant* exits.

Exporting SSO Settings

1. Run the *Single Sign-On Assistant*.
2. Click **Export**.
3. Browse to the file to export the settings to, and then click **Save**.
4. Click **OK** when the *Single Sign-On Assistant* reports successful export.

Chapter 7
Configuring Default System and User Policy

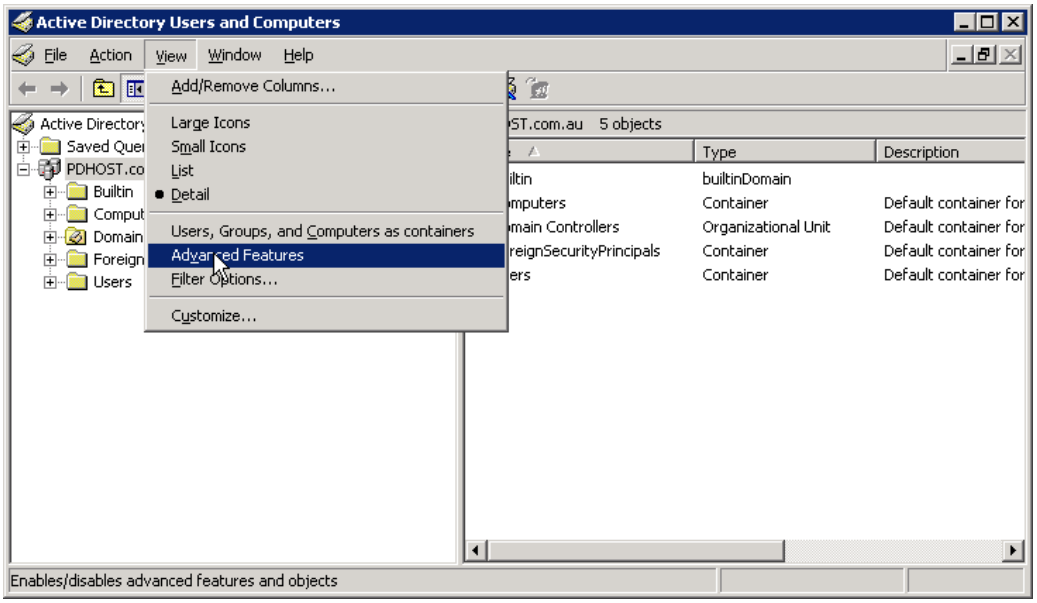
ProtectDrive will store an instance of a Default System and User Policy in Active Directory/ADAM. Every time a new computer account is created in the Windows Domain, these stored default settings will automatically apply.

Clients that are managed by the property sheet of their own computer object are managed through the **ProtectDrive Management Console**, via the **Active Directory Users and Computers (ADUC)** MMC snap-in. Clients that are linked to either the Default Configuration Object or another Configuration Object are managed through the **ProtectDrive Management Console**, via the **ProtectDrive Management Console** snap-in.

Configure Default Settings in Active Directory Users and Computers (ADUC) MMC Snap-in

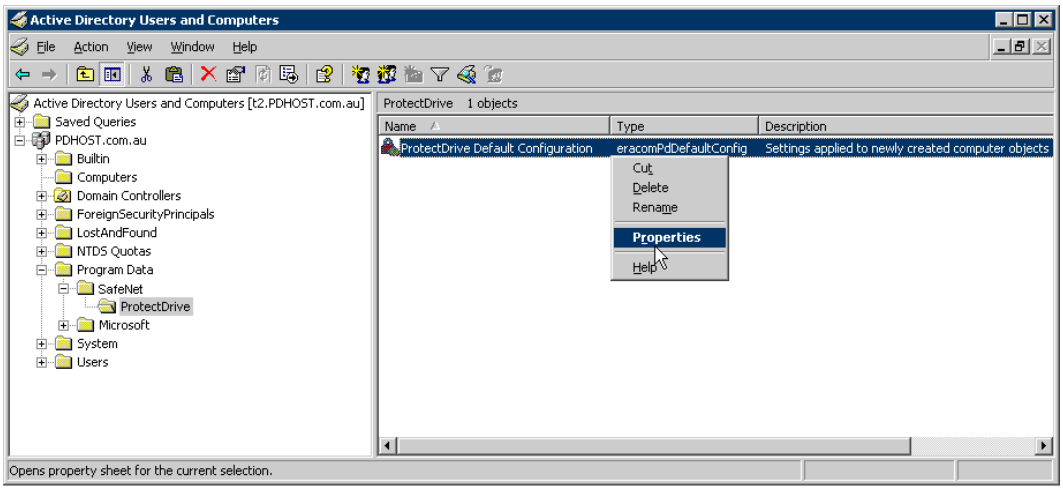
The ADUC MMC snap-in is primarily used for initial ProtectDrive configuration immediately after ProtectDrive is installed. For subsequent configuration changes, use the ProtectDrive Management Console.

1. On the server, open the **ProtectDrive Management Console**.
2. Open the **Active Directory Users and Computers** MMC snap-in.
3. Select **View > Advanced Features**.



© SafeNet, Inc.

4. Navigate to **Program Data > SafeNet > ProtectDrive > ProtectDrive Default Configuration** and select **Properties**.



5. Click the **PD Settings** tab, and then configure the default System Policy. Refer to page 109 for details on the **PD Settings** selections.

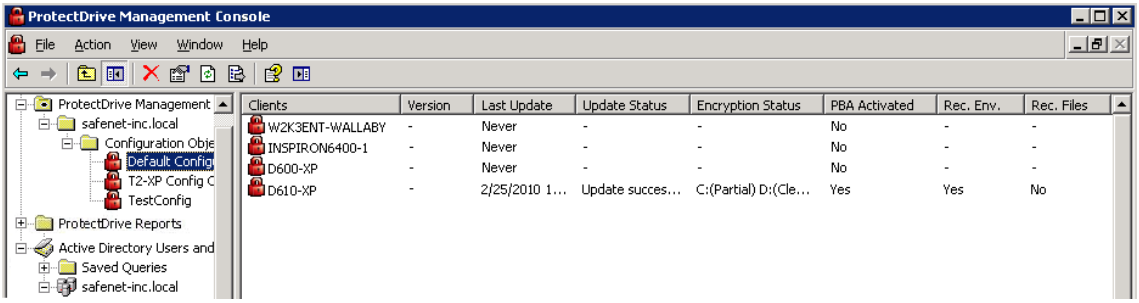
6. Click the **PD Users** tab, and then assign users to the system by default, and to configure these users' device access control permissions. Refer to page 129 for details on **PD Users** selections.

7. Click **Apply**.

8. Click **OK**.

Configure Default Settings in ProtectDrive Management Snap-in

1. On the server, open the **ProtectDrive Management Console**.
2. Select **ProtectDrive Management > Configuration Objects**.

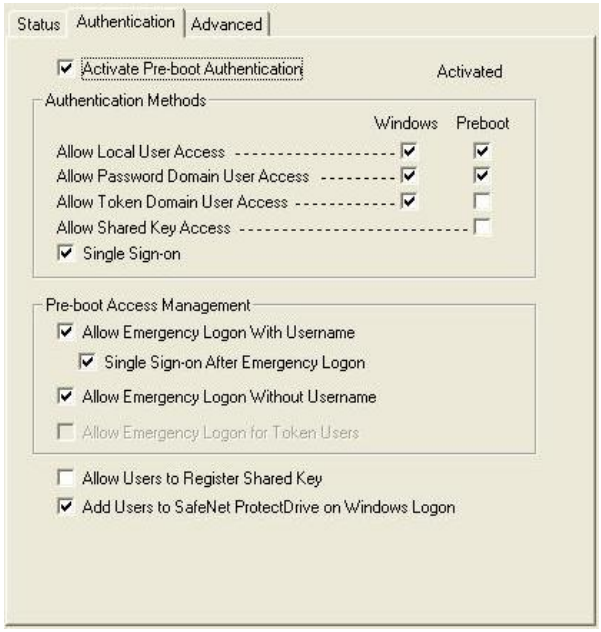

ProtectDrive Management Console
File Action View Window Help
ProtectDrive Management
safenet-inc.local
Configuration Obje
Default Config
T2-XP Config C
TestConfig
ProtectDrive Reports
Active Directory Users and
Saved Queries
safenet-inc.local
Clients Version Last Update Update Status Encryption Status PBA Activated Rec. Env. Rec. Files
W2K3ENT-WALLABY - Never - - No - -
INSPIRON6400-1 - Never - - No - -
D600-XP - Never - - No - -
D610-XP - 2/25/2010 1... Update succes... C:(Partial) D:(Cle... Yes Yes No

3. Right-click on the ProtectDrive **Default Configuration**, and then select **Properties**.
4. Click the **PD Settings** tab, and then configure the default System Policy. Refer to page 109 for details on the **PD Settings** selections.
5. Click the **PD Users** tab, and then assign users to the system by default, and to configure these users' device access control permissions. Refer to page 129 for details on **PD Users** selections.
6. Click **Apply**.
7. Click **OK**.

© SafeNet, Inc.

PD Settings Tab – Configure the Default System Policy

Authentication Settings



Activate Pre-boot Authentication

This check box must be selected for ProtectDrive to provide disk encryption and pre-boot authentication on the client.

To disable ProtectDrive without uninstalling it, clear this check box. All aspects of ProtectDrive, including disk encryption, will be disabled. If this check box is cleared, changes to other settings on the **Authentication** tab can be made, but the settings do not take effect until ProtectDrive is enabled by selecting the **Activate Pre-boot Authentication** check box again. Check the activation status by referring to the **Activated / Pending / Deactivated** indicator, located to the right of the **Activate Pre-boot Authentication** check box. An example is shown below.

The status messages that may display are:

Active	Pre-boot authentication is turned on.
Pending	The server is waiting for the client to update to the state that is currently set on the server.
Deactivated	Pre-boot authentication is turned off. When deactivated, previously encrypted drives will be decrypted. When **reactivated**, ProtectDrive resets all user passwords to the configured initial pre-boot password, which may be explicitly defined in **PD Settings > Advanced > Password Policy**, where the default password is set to be equal to the username, or set to a designated default (the pre-set default is "*password*").

Deactivating **Pre-boot Authentication** will remove all users from the client system's ProtectDrive Pre-boot User database. When **Pre-boot Authentication** is reactivated, all users (Windows Domain users and local Windows users) will be re-added automatically.

Authentication Methods

To gain access to a system protected by ProtectDrive, authentication at both the Pre-boot and Windows access levels is mandatory.

One or a combination of local user, password domain, and token domain authentication methods will be available to users at the Pre-boot and Windows access levels, as determined by the settings made in the **Authentication Methods** group box. These authentication methods are described in detail below.

To make an authentication method available to users, select either the **Windows**, the **Pre-boot**, or both check boxes next to the method, according to the security policy requirements that apply in the organization. At least one check box must be checked at both the **Windows** and **Pre-boot** levels across the authentication methods.

If you do not have any tokens (the drivers are not installed) to log on to Windows, do not configure ProtectDrive to only allow Windows logon/authentication using tokens (and smart cards). If you configure ProtectDrive in such a way, and the PC is locked, there is no way to unlock it with a password since ProtectDrive is configured to only allow token logons. The administrator should ensure there is a valid token to be used for both PBA and Windows logon (and unlocking) before configuring ProtectDrive for token only access.

© SafeNet, Inc.

Allow Local User Access	Enabled by default, this method allows the Local Windows users to authenticate into the system using their Local Windows Username, Password, and Local System Name. Local Windows users can only be added using the **Local Management Console** utility, or via a Windows Logon when **Add Users to SafeNet ProtectDrive on Windows Logon** is set at the bottom of this **Authentication** screen. Local Windows users can **not** be added to the client system's user database from the server.
Allow Password Domain User Access	This method allows the Windows Domain users to authenticate into the system using their Windows Domain User Name, Password, and Domain Name.
Allow Token Domain User Access	This method enables Windows Domain users to use a smart card/token and PIN/fingerprint for authentication.
Allow Shared Key Access (for iKey 1000 users only)	This method allows pre-boot authentication for a token shared key (*non-PKI*) user. If this option is selected, at least one **Windows** authentication method must be selected as well.

Notes About Token Domain User Access as the Sole Authentication Method

Caution must be taken if **Allow Token Domain User Access** is the only enabled authentication method.

If the following options are all disabled, then smart cards/tokens are the only means of authentication into the system at pre-boot:

- **Allow Local User Access**
- **Allow Password Domain User Access**
- **Allow Emergency Logon Without Username**

If any problems with the smart cards/tokens are encountered, the system may be rendered inaccessible. For this reason, it may be a good idea to temporarily enable the **Allow Local User Access,** and/or the **Allow Emergency Logon Without Username**, and/or the **Allow Emergency Logon for Token Users** options. This will allow for at least one alternative method of Pre-boot authentication until the smart cards/tokens are proven to be reliable and properly set up for use with ProtectDrive.

Single Sign-on

In single sign-on mode, a user need only log in once to authenticate at both the Pre-boot and Windows levels. This option is available only when authentication at both the Pre-boot and Windows access levels is enabled for at least **one** authentication method.

Single sign-on is currently not supported with fingerprint logon.

Select the **Single Sign-on** check box to enable single-sign on mode.

Pre-boot Access Management

The **Pre-boot Access Management** settings are available when authentication is enabled at the **Pre-boot** level when the **Allow Local User Access** and/or **Allow Password Domain User Access** check boxes are selected.

The **Pre-boot Access Management** settings are described below.

Allow Emergency Logon With Username

When enabled, this option allows the user to invoke the *Emergency Logon With Username Procedure*. It is used in cases where the user has forgotten their pre-boot authentication password (not a PIN). This includes Windows Domain or Local Windows user password accounts that have been added to ProtectDrive.

It allows for one-time-only pre-boot access to the system.

This feature will require a user to successfully log in through Pre-Boot Authentication before it can be invoked by that user.

Single Sign-on After Emergency Logon

When enabled, this option allows the user to automatically authenticate post-boot into Windows immediately following successful exercise of the *Emergency Logon With Username Procedure*.

With the **Pre-boot Access Management** group box enabled, this option becomes available for selection when authentication is enabled at the *Windows* level if the **Allow Local User Access** and/or **Allow Password Domain User Access** check boxes is/are selected.

Single sign-on is currently not supported with fingerprint logon.

© SafeNet, Inc.

Allow Emergency Logon Without Username	When enabled, newly created Windows Domain or Local Windows users may invoke the *Emergency Logon Without Username Procedure*. This allows for one-time-only pre-boot access to the system for all users who do not yet have a ProtectDrive Pre-boot user account.
Allow Emergency Logon for Token Users	(This option is available only if at least one of the following **Pre-boot** Authentication Method options is selected: **Allow Token Domain User Access** or **Allow Shared Key Access**.) If this option is enabled, smart card/token users (who have misplaced their token or forgotten their PIN) are permitted to invoke the *Emergency Logon for Token Users Procedure*. This procedure allows for a one-time-only pre-boot access to the system without the need of a token.

Allow Users to Register Shared Key

When this option is enabled, users are allowed to register a shared key for authentication.

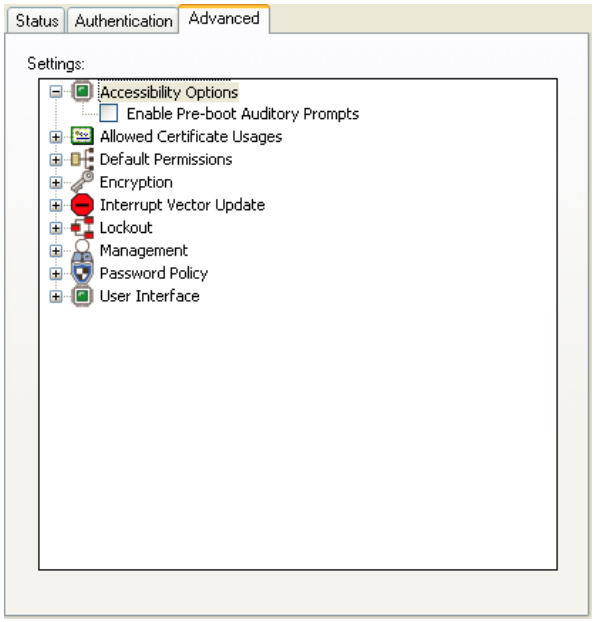
In addition, this option must be enabled to display the **Shared Key** menu selection (shown right) when the ProtectDrive icon in the notification area is opened.

Add Users to SafeNet ProtectDrive on Windows Logon

When this option is enabled, a new ProtectDrive pre-boot user account will be created (if it does not already exist) for a user when they logon to Windows.

This functionality depends on the settings of the **Allow Local User Access**, the **Allow Password Domain User Access**, and the **Allow Token Domain User Access** options. An entry will be created for the user in the ProtectDrive Pre-boot User database only if a setting that corresponds with the ~~–t~~ype" of Windows logon being performed is set.

Advanced Settings – Accessibility Options



Enable Pre-boot Auditory Prompts

Auditory prompts are intended to be used by visually impaired users. When this feature is enabled, audio prompts will occur for a number of screen states or conditions during the pre-boot login process.

The auditory prompting feature can also be toggled on and off by pressing **F3** from any pre-boot login screen.

Each audio prompt consists of a series of short or long beeps, or a combination of both. Refer to the table on the next page for a description of each audio prompt and the condition under which it will occur.

Audio prompting is available on 32-bit pre-boot user authentication only (it is not supported for legacy pre-boot authentication).

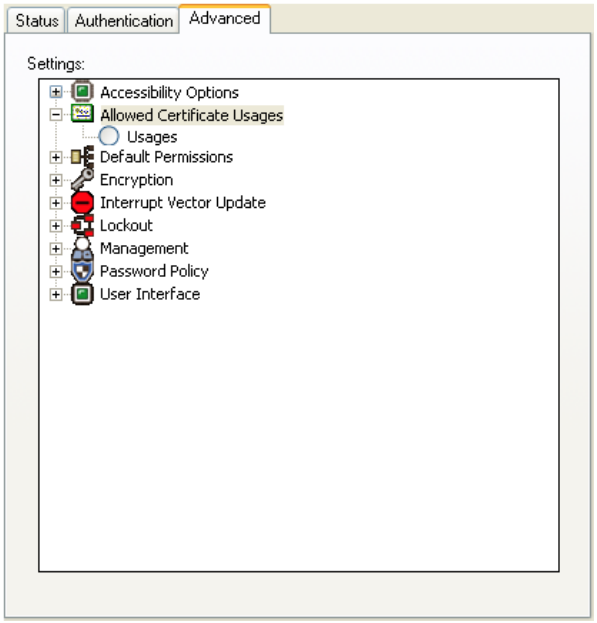
When audio prompting is enabled, press **F4** to replay the audio prompt for the current field or condition.

If the user is unable to determine where they are in the login process, press **Esc** to return to the initial pre-boot screen. (This is only applicable if both password and token authentication methods are enabled.)

© SafeNet, Inc.

This pre-boot prompt, state, or condition…	…emits this audio prompt…	…which equates to these musical notes…	…and you should:
Insert the smart card/token or press Enter (**Note**: This screen displays only if both password and token authentication methods are enabled. If only one method is enabled, the first audio prompt the user hears will either be for user name entry, which is 2 short beeps, or for PIN entry, which is 3 short beeps.)	1 long beep	A	Insert a smart card/token or press **Enter** to continue.
Enter the user name (User ID)	2 short beeps	B, B	Enter your user name and press **Tab** to continue.
Enter the password	3 short beeps	C, C, C	Enter your password and press **Tab** to continue.
First domain in the list is selected	4 short beeps	D, D, D, D	Press **Enter** to select the first domain in the list to continue, or press the down arrow to select a different domain.
Press the up/down arrow to choose a different domain (**Note**: One short beep will occur with every press of the up/down arrow. If the first domain is reached again, 4 short beeps will sound to indicate the user is at the top of the domain list.)	1 short beep	E	Press **Enter** to continue.
Enter the PIN	3 short beeps	C, C, C	Enter your PIN and press **Enter** to continue.
Logon is successful	1 long beep, 3 short beeps	G, D, B, A	None
A pop-up box is displayed, as a result of the user's last action. The pop-up box describes feedback such as: • A general entry error occurred (for example, an invalid user name, password, PIN, smart card, or bad certificate). • The user pressed **F1** which displays a login help screen	1 short beep, 1 long beep	B, D	Press **Enter** to clear the pop-up box and continue. • If the condition occurred while entering a user name or password, continue by re-entering that information. • If the condition occurred while entering a PIN, continue by re-entering a correct/valid PIN, or by replacing the card with one that works.
Challenge/response screen is active	2 long beeps	A, A	Contact your administrator for recovery instructions.
Lockout screen is displayed The user has reached the number of failed log in attempts and is now locked out for a period of time.	2 beeps, 1 long beep	B, B, F	Press **Enter** to acknowledge the message and wait the configured amount of time to attempt login again.
Critical/fatal error	3 short beeps, 1 long beep	B, B, B, F	Contact your administrator.

Advanced Settings - Allowed Certificate Usages



This option is used to configure the acceptable certificate usages that are allowed for token or smart card pre-boot logon.

Usages

Click the **Usages** option to display the currently available certificate usages. The name and object identifiers (OIDs) of each certificate usage displays. OIDs are the numeric values that enable programs to determine whether a certificate is valid for a particular use, such as pre-boot authentication.

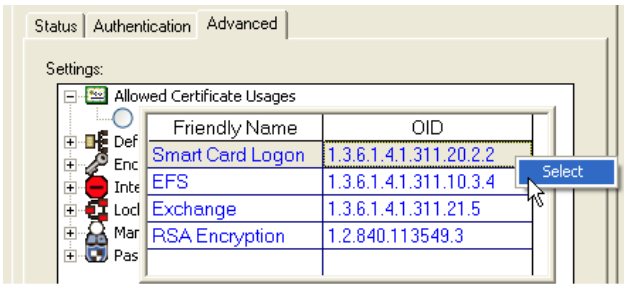
By default, the following certificate usages are available:

- **Smart Card Logon**—Select this usage type to allow smart card logon to Windows.
- **EFS**—Select this usage type to allow third-party certificate authority support for encrypting file systems.
- **Exchange**—Select this usage type to allow a private key or a certificate authority.
- **RSA Encryption**—Select this usage type to allow this algorithm for Windows encryption.

Enable any (or all) of these usages, or manually add more certificate usages as needed. Certificate usages that are enabled are highlighted in gray.

© SafeNet, Inc.

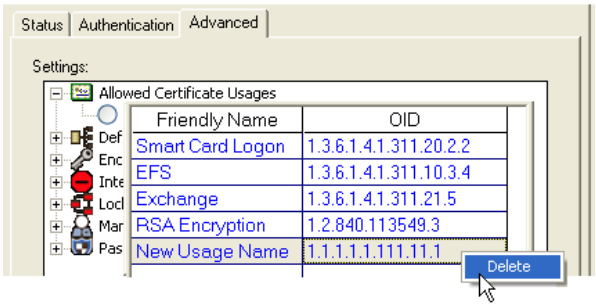
- To allow an existing certificate usage, right-click on its name or corresponding OID, and then choose **Select**. Once it is selected, the background will turn gray.



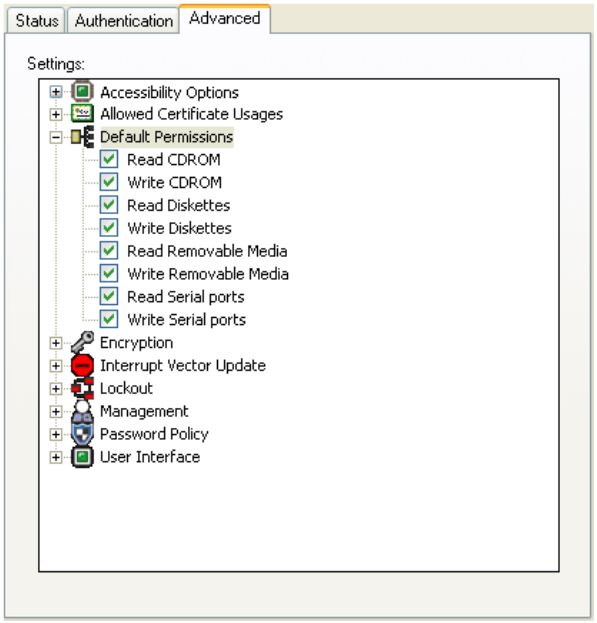
- To disallow an existing certificate usage, right-click on its name or corresponding OID, and then choose **Unselect**. Once it is de-selected, the background will turn white.

- To manually add a certificate usage, double-click inside the blank row at the bottom of the list, enter the name and OID, and then press **Enter**. (A new blank row is automatically created.) Any item that is manually added is automatically allowed (highlighted in gray).

- Manually added items cannot be de-selected—they can only be deleted. To delete a manually added certificate usage, right-click on the name or OID, and then click **Delete**.



Advanced Settings - Default Permissions (Device Access)



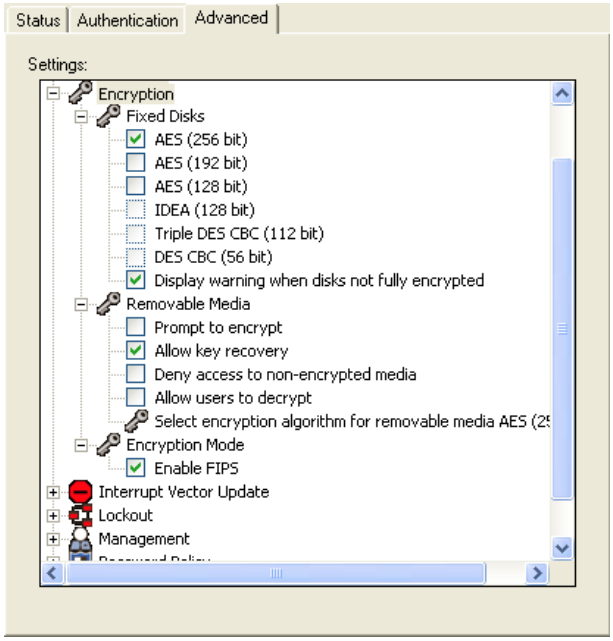
Default Permissions only apply to users whose individual User Policy has not yet been defined explicitly on the **PD Users** tab. In fact, individual User Policy settings that are defined in the **PD Users** tab will override these Default Permissions.

For example, a user may be added to the ProtectDrive pre-boot user database following a successful Windows login (see the **Add Users to SafeNet ProtectDrive on Windows Logon** option on the **Authentication** tab.)

If this user was not explicitly added to the system using the **PD Users** tab, then their device access permissions to the systems resources will be governed by the settings in the **Default Permissions** group.

© SafeNet, Inc.

Advanced Settings - Encryption



Fixed Disks

Choose the encryption algorithms to be made available to users during ProtectDrive encryption. The algorithms that you choose here will display as algorithm selections in the **Encryption Status** group.

The **IDEA**, **Triple DES CBC,** and **DES CBC** options are unavailable if the **Encryption Mode > Enable FIPS** option is selected.

Display warning when disks not fully encrypted

This option is enabled by default. It displays a ProtectDrive balloon tip to all users, to inform them of an incomplete disk encryption status. This ProtectDrive warning message displays immediately after Windows logon. Refer to page 181 for an example.

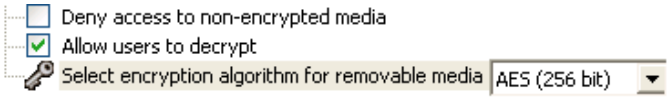
Removable Media

Choose the options that will apply to all removable media:

Prompt to encrypt	If enabled, when unprotected (non-encrypted) removable media is inserted, the user is prompted whether or not to encrypt the media.
Allow key recovery	If enabled, the system will allow a user to regain access to the protected removable media in the event of a forgotten password.
Deny access to non-encrypted media	If enabled, the system denies access to any removable media that is not encrypted. If removable media is connected when this option is set, safely remove the device and then reconnect it for the setting to take effect.
Allow users to decrypt	(If the **Deny access to non-encrypted media** option is selected, this option not available.) When enabled, this option allows a user to decrypt a removable media component.

Select encryption algorithm for removable media

Click on this option, and then choose the encryption algorithm to use during ProtectDrive encryption of removable media.



The **IDEA**, **Triple DES CBC**, and **DES CBC** options are unavailable if the **Encryption Mode > Enable FIPS** option is selected.

Encryption Mode

Choose the **Enable FIPS** check box to use the FIPS mode library. If this option is selected, the fixed disk and removable media IDEA, Triple DES CBC, and DES CBC encryption algorithm options are not available. If this option is selected on ProtectDrive clients on Windows 7 (64-bit version) or Windows Server 2008 R2 platforms, ProtectDrive will use the Microsoft Cryptographic Primitives Library (**CNG**), which in turn, operates in its FIPS mode of operation only when one of the following DWORD registry values is set to 1:

- HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled

  --or--

- HKLM\SYSTEM\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration\SelfTest Algorithms

To ensure ProtectDrive's operation in FIPS-approved mode, you should pre-configure one of these registry values on your system.

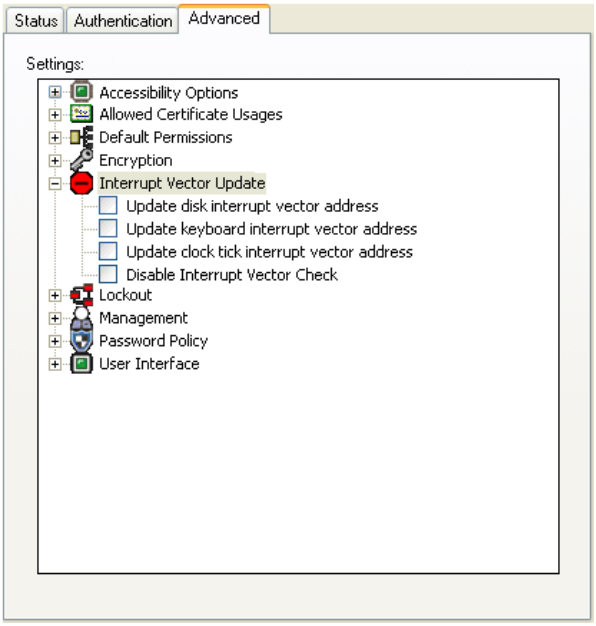
© SafeNet, Inc.

For additional details, please refer to the following Security Policy document: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1328.pdf.

If the **Enable FIPS** option is **not** selected, performance is enhanced and a secure, Common Criteria EAL-4 approved, non-FIPS library is used.

If you change the status of this option, you must reboot the client for the change to take effect.

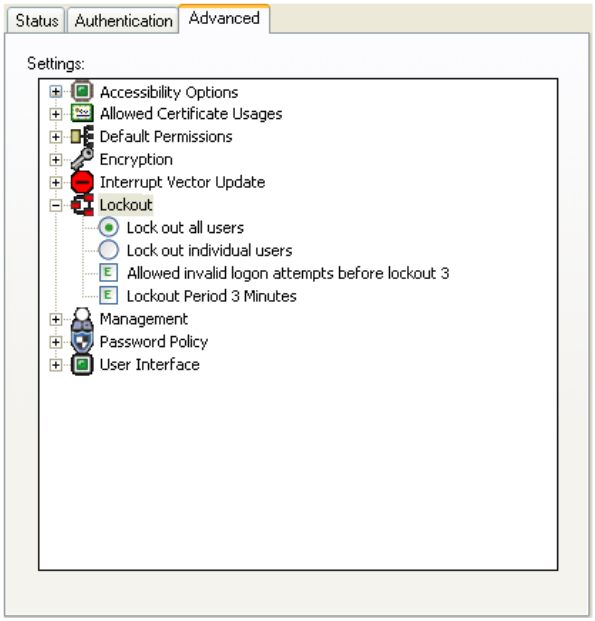
Advanced Settings - Interrupt Vector Update



ProtectDrive maintains a store of some of the BIOS interrupt vector addresses. This allows ProtectDrive to detect potential attacks mounted by the changing of the interrupt vector address. When ProtectDrive detects a difference between the BIOS interrupt vector address and the copy held by ProtectDrive, an error message displays.

When interrupt vector addresses change (for example, updating the BIOS) this error message is still displayed. The **Interrupt Vector Update** group provides a mechanism to accept a legitimate change by updating ProtectDrive's copy of the disk, keyboard, and clock tick interrupt vector address, as well as a means to disable the interrupt vector check.

Advanced Settings - Lockout



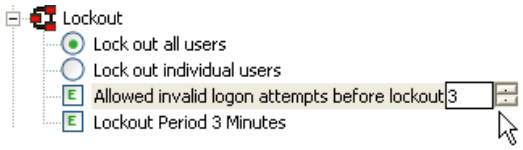
The **Lockout** group is used to prevent password guessing attacks. After a number of failed logon attempts, further logon attempts are prevented for a configurable period of time. (Open the system's **Event Viewer** for details on failed logon attempts and other events. See page 184 for more on **Event Viewer**.)

Lock out all users / Lock out individual users

These settings determine whether access to all or individual user accounts is blocked for a period of time after too many failed logon attempts. The default is **Lock out all users**.

Allowed invalid logon attempts before lockout

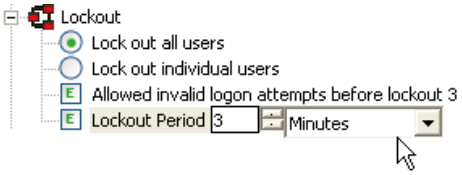
ProtectDrive will lock a computer after the specified number of unsuccessful logon attempts at the pre-boot logon screen has occurred. Click in this field, and then select the desired number of attempts. The default value is three (3).


Lockout
Lock out all users
Lock out individual users
Allowed invalid logon attempts before lockout 3
Lockout Period 3 Minutes

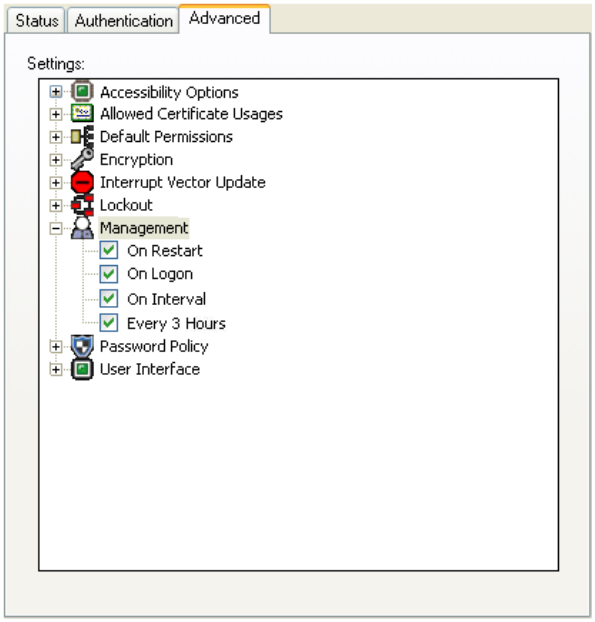
© SafeNet, Inc.

Lockout period

This value determines the length of time that access to the system or an individual account is blocked. Click in this field and then select the desired lockout period. The default setting is three (3) minutes. The maximum lockout period is 365 days.



Advanced Settings - Management



This group configures how the ProtectDrive client retrieves System and User Policy data (for example, updated information) from Active Directory/ADAM.

These options will display as inactive on the client if this was a **Client Configuration** installation.

On Restart

If this check box is selected, the ProtectDrive client pulls policy data from the Active Directory/ADAM service on Windows login.

On Logon

If this check box is selected, the ProtectDrive client pulls policy data from the Active Directory/ADAM service on user login.

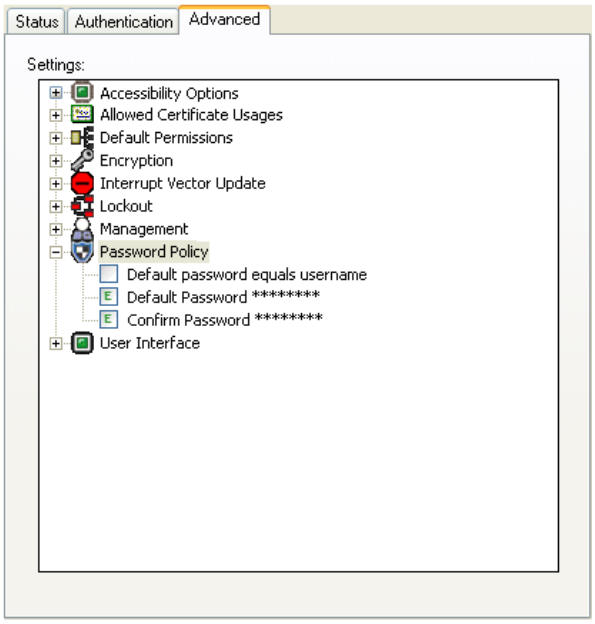
On Interval

If this check box is selected, the ProtectDrive client pulls policy data from the Active Directory/ADAM service based on the specified number in the **Every __ Hours/Days** field.

Every __ Hours/Days

Click in this field, and then select the desired interval that the ProtectDrive client pulls policy data from Active Directory/ADAM.

Advanced Settings - Password Policy



© SafeNet, Inc.

Default password equals username

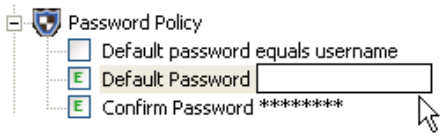
This option is an alternative to specifying the Default Password. Note that in this case, the users still need to type in their password (their Windows Username) for pre-boot authentication.

Note that when the password is the user's name, it is only used for the initial (first time ever) pre-boot authentication, and is then replaced by the Windows (Domain) password.

Windows passwords must also be limited to a maximum length of **127** characters.

Default Password / Confirm Password

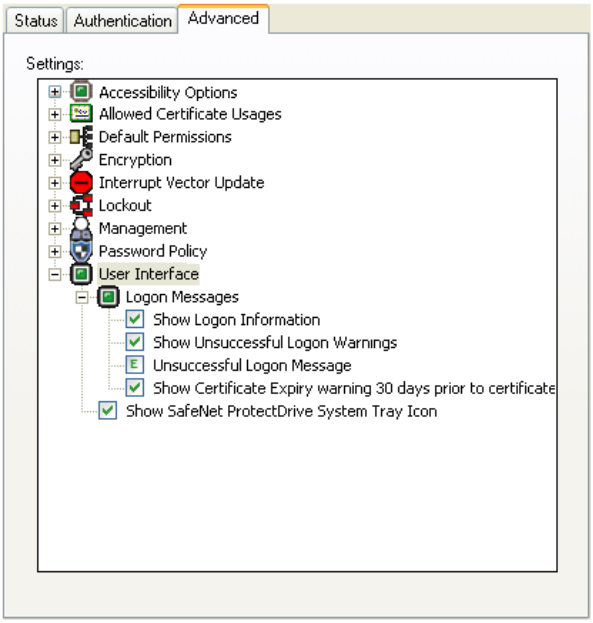
This field defaults to "**password**." To change the password, click the **Default Password** check box, and then enter the new password. Repeat this procedure in the **Confirm Password** check box.



Newly added Windows (Domain) users may be instructed to enter the Default Password for their initial (first time ever) pre-boot authentication. Once the user authenticates into Windows using their actual Windows (Domain) password, the ProtectDrive Default Password will be *replaced* with the user's Windows (Domain) password in the ProtectDrive Pre-boot User database.

Windows passwords must also be limited to a maximum length of **127** characters.

Advanced Settings - User Interface



Show Logon Information

By default, the *SafeNet ProtectDrive Logon Information* balloon tip displays immediately before the Windows Explorer Shell loads. This message shows the date and time of the last successful logon, the date and time of the last password change, and the number of successful logons. Clear this check box to disable displaying of logon information. Refer to page 182 for an example.

Show Unsuccessful Logon Warnings

By default, a ProtectDrive balloon tip displays if previous unsuccessful pre-boot authentication attempts have occurred. This warning is displayed immediately preceding the loading of the Windows Explorer Shell. Clear this check box to disable the display of this balloon tip. Refer to page 182 for an example.

Unsuccessful Logon Message

When the **Show Unsuccessful Logon Warnings** option is selected, an optional message can also be displayed by entering this message in the **Unsuccessful Logon Message** field.

Show Certificate Expiry warning 30 days prior to certificate expiry

If this option is selected, smart card/token users will see a warning the specified number of days before their certificate expires.

© SafeNet, Inc.

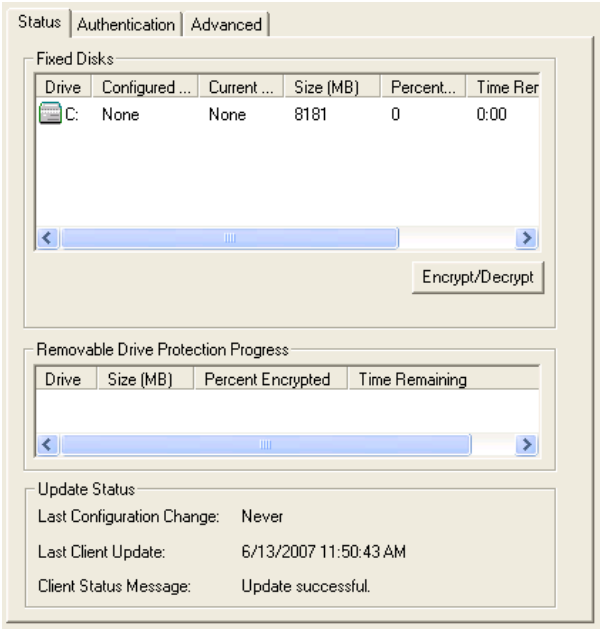
Show SafeNet ProtectDrive System Tray Icon

After ProtectDrive is installed, a small ProtectDrive icon is placed in the Windows notification area of the taskbar, located in the lower-right corner of the Windows desktop. This icon can be disabled by clearing the **Show SafeNet ProtectDrive System Tray Icon** check box.

When this option is enabled, right-click on the icon, and then choose one of the following:

- **Local Management Console**—Open the Local Management Console (you can double-click on the icon to open LMC as well).
- **Lock Computer**—Lock the Windows desktop. (This option is not available if ProtectDrive is installed on Windows Vista or Windows 7).
- **Shared Key**—Manage the user's shared key. This option will display only if the **Allow Users to Register Shared Key** option is selected in **PD Settings > Authentication**.
- **About SafeNet ProtectDrive**—View the ProtectDrive version, license, and copyright information.

Status Settings



The **Status** group allows for default configuration and automatic execution of disk encryption on the remote client system. Any partitions configured for encryption here will be automatically encrypted by default on all systems newly added to the Windows Domain.

The **Update Status** section of this screen includes the date, time, and status of the last client update and/or client configuration change.

Drive

This column lists all possible partitions for the client system. Note that this list does not accurately portray the partition allocation table on the client system. Since this information is not readily available in Active Directory/ADAM, ProtectDrive will first list all possible partitions between C and Z. Then, after the first successful update, only the drives that actually exist on the client will display. When viewing the client computer from the **Local Management Console**, however, the existing drives are always the only ones that display.

Configuring default encryption on a partition letter that does not actually exist on a particular client will result in no negative consequence.

Configured Algorithm

This column lists the algorithm selected for the encryption of the given partition. If **None** is shown, the partition is either not configured for encryption or (if already encrypted, see the **Current Algorithm** column) it is slotted for decryption.

For each partition that you wish to encrypt by default, click the **Encrypt/Decrypt** button, and then choose an algorithm from the list that displays. If a particular algorithm does not display in this list, check the **Encryption** group.

Current Algorithm

This has no effect on the default configuration. In general, this column represents the encryption status of the partition. If **None** is shown, then the partition is not currently encrypted.

Removable Drive Protection Progress

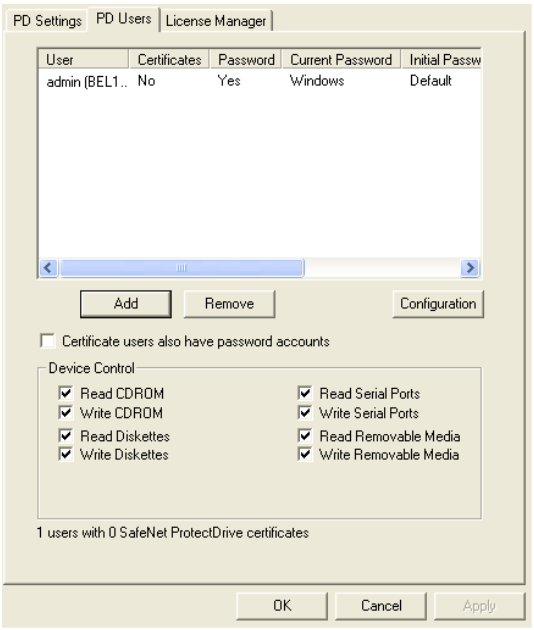
This window displays the progression of an encryption or decryption operation of the removable media. A drive letter and progress bar will display only if the operation is started prior to opening the **PD Settings > Advanced > Status** group, or while that screen is open.

© SafeNet, Inc.

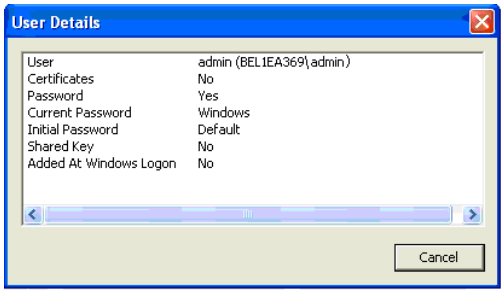
PD Users Tab – Configure the Default User Policy

By using the options on the **PD Users** tab, certain Windows Domain users can be automatically assigned to newly created computer objects. Device access control permissions for these users can also be configured here.

Device access control permissions that are defined on this tab will *override* the system settings in the **PD Settings > Advanced > Default Permissions** group.



Tip: To view a user's current settings at a glance, double-click on their name. The *User Details* window displays.



User

This column lists individual domain users and groups of users which will be automatically assigned to all newly created computer objects in the given domain. Click **Add** or **Remove** to populate this column from Active Directory/ADAM.

Certificates

The settings for this column are **Yes** or **No**. If the column indicates **No**, the user does not have any certificates. If a column indicates **Yes**, the number of valid smart card/token certificates the user possesses in the given domain is also shown.

Users with certificates are able to log into ProtectDrive using their smart card/token. Note that the total number of assigned certificates is also listed at the bottom of the **PD Users** tab.

A ProtectDrive User account is created for each smart card/token certificate. Including any accounts created for password users, the total number of accounts on each client system cannot exceed **2000**.

Password

The settings for this column are **Yes** or **No** to indicate whether or not a user or all members of a Windows group possesses an initial password account to log into ProtectDrive.

The **Password** column displays **Yes** if:

- A user with certificate(s) is assigned a password via the use of the **Configuration** button.
- A user with a password account only is added.
- A certificate user is added and the **Certificate users also have password accounts** check box is selected.

The **Password** column displays **No** if:

- A certificate user is added and the **Certificate users also have password accounts** check box is **not** selected.

Current Password

The settings for this column are **Initial** or **Windows**. This column indicates the user's current password.

By default, this setting will display as **Initial** for users who have been manually added in ProtectDrive, and who have not yet authenticated into Windows using their actual Windows (Domain) passwords. After logging into Windows, the user's pre-boot authentication password is synchronized with their Windows password, and the setting is replaced with **Windows**.

© SafeNet, Inc.

Initial Password

The settings for this column are **Set** or **Default**. This column indicates whether the user's initial password was specified by the administrator (**Set**) or if the default password is being used (**Default**). The number of password users and smart card/token certificate users should not exceed **2000**. Passwords are assigned by using one of these methods:

- To specify a user's password, highlight the user's name, and then click the **Configuration** button. De-select the **Use default password** check box, and then enter and confirm a unique password for the selected user/group. Setting a specific password will *always* override the default password. The **Password State** will now be changed to **Set**.

- To use the default password, highlight the user's name, and then click the **Configuration** button. Select the **Use default password** check box. The default password assigned to the user will be the one that is defined in the **PD Settings > Advanced > Password Policy** group.

- To give all certificate users (including group members) password accounts, select the **Certificate users also have password accounts** check box. This will assign the default password (as defined on the **Password Policy** group) to all users who do not have a password assigned. (A user's default password can be changed to a specific one later on by using the **Configuration** button described above.)

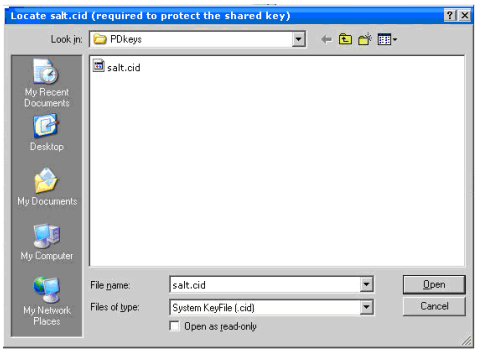
Shared Key

This column indicates whether or not a user has a registered (generated) shared key for pre-boot authentication. (A shared key can be registered from the **LMC** or the **Active Directory Users and Computers** MMC snap-in.) A user with a shared key can log into ProtectDrive using a shared key token (iKey 1000).

To register a shared key:

1. Click on the user's name.
2. Click the **Shared Key** button.
3. Insert the shared key token, and then click **OK**.

4. Enter the PIN, and then click **OK**.
   - If the token has not been initialized, a new shared key is created on the token.
   - If an existing shared key is detected on the token, you are prompted whether or not to use that shared key.
     - Choose **No**, and then choose **Yes** to overwrite the shared key.
     - If you are configuring the shared key **locally** (from the LMC), the procedure is complete. A message will display to indicate that the key has been updated.
     - If you are configuring the shared key from the ProtectDrive **server** (from the Active Directory Users and Computers MMC snap-in), you are prompted for the **salt.cid** file. Proceed to step 5.
5. Navigate to and select the **salt.cid** file, and then click **Open**.



A message will display to indicate that the key has been updated.

A shared key can also be registered to a user through the **Shared Key** option accessible from the SafeNet ProtectDrive notification area icon, located in the lower-right corner of the Windows desktop.

Added at Windows Logon

This column indicates whether or not a user is automatically added to the ProtectDrive database when the user logs into Windows. If the user does not already exist in the ProtectDrive database, and the **Add Users to SafeNet ProtectDrive on Windows Logon** option is selected (on the **PD Settings > Authentication** tab), then the user is added to ProtectDrive after logging into Windows.

Device Control

The settings in this section are used to define the default read and write permissions to the devices listed for each user (or group) in this tab. The **Write** setting for each device can only be enabled if the **Read** setting is also enabled. Make sure you click **Set** to save these settings in Active Directory/ADAM—clicking **OK** or **Apply** will **not** save these permissions in Active Directory/ADAM.

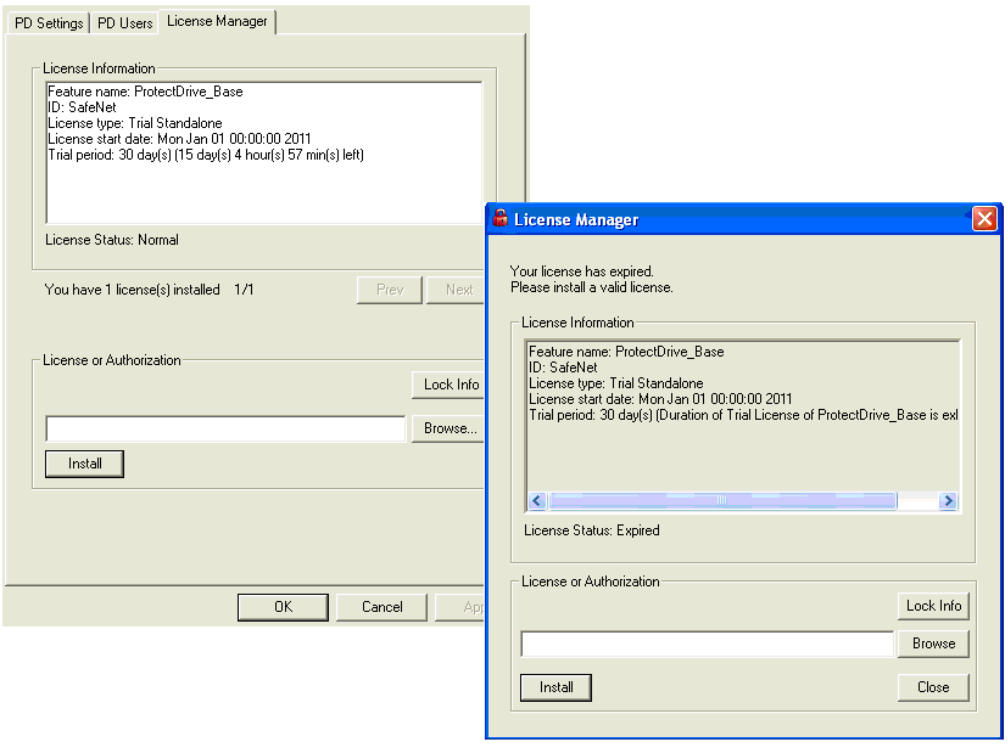
© SafeNet, Inc.

License Manager Tab – View/Install/Update License

ProtectDrive ships with a 30-day evaluation (trial) license. The trial license or full license is installed during the ProtectDrive installation. You must have a valid license to install a full license. Features (for example, Removable Media) are enabled or disabled based on the installed license or authorization code.

The **License Manager** tab in the Local Management Console displays information about the ProtectDrive license(s) that are currently installed. After ProtectDrive is installed, use the **License Manager** tab (shown below, left) to upgrade from the trial version, or upgrade an expired license.

When a license expires, a ~~n~~ag" screen (shown below, right) will continue to display periodically until a valid license is installed.



Any time the license changes, it is good practice to run the backup.exe utility to ensure your recovery files are up-to-date. Refer to Chapter 11 for details on the backup utility.

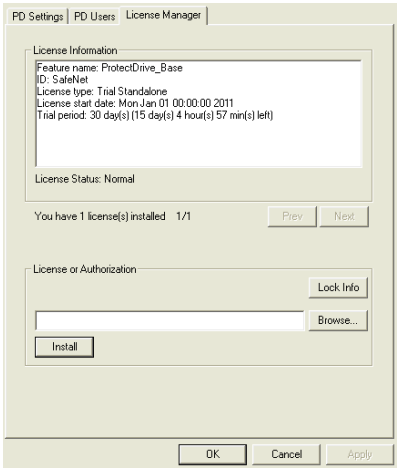
Upgrade to a Full License From License Manager

You can upgrade your license if you currently have a trial license installed, or your license has expired. Before you begin, make sure you have a valid **license.txt** (for a single client installation) or **authorization.txt** file (for locked licensing for multi-license client installations) stored in a location that the client PC can browse to during the upgrade procedure.

Client PCs should have Internet access to complete a locked license installation. Refer to page 11 for licensing details.

1. From the Windows desktop, right-click on the ProtectDrive icon in the notification area, and then select **Local Management Console**, or simply double-click on the icon.

2. Click the **License Manager** tab.



3. Perform one of the following:
   - Browse to the **license.txt** file, and then click **Install**.
   - Browse to the **license.txt** file, and then open it. Copy and paste the entire block of text into the blank field and then click **Next**.
   - Browse to the **authorization.txt** file, and then click **Next**.
4. If you are using the **authorization.txt** file to receive a license, the client will now contact the license server. If successful, the license server will send a locked license to the client.

5. A message will display if the license update was a success.

Upgrade to a Full License From the Nag Screen

From the nag screen, perform steps 3 through 5 detailed in the previous section.

© SafeNet, Inc.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 8
System and User Management

ProtectDrive clients are managed centrally from the **ProtectDrive Management Console**, on the server with the System and User Policy data stored in and replicated from Active Directory/ADAM.

The **Active Directory Users and Computers** MMC snap-in is amended with the **PD Settings** and **PD Users** tabs, and is used to manage ProtectDrive clients with their own unique configuration policies.

The **ProtectDrive Management** snap-in is virtually the same as the **Active Directory Users and Computers** MMC snap-in—it has the **PD Settings** and **PD Users** tabs—but it is used to manage groups of ProtectDrive clients with the same configuration policy.

Alternatively, the **Local Management Console** utility may be used to manage clients locally. Local configurations may be saved in Active Directory/ADAM. Each client reports updated policy data back to the server.

Manage System Policy From the Server

Before configuring System and User Policy, review the contents of Chapter 7 –Configuring Default System and User Policy. This will familiarize you with the fields on the **PD Settings** tabs. These tabs are used to configure ProtectDrive System Policy.

All systems in a Windows Domain can be managed remotely with the use of the **PD Settings** and **PD Users** tabs in the **ProtectDrive Management Console** snap-ins. The configuration settings in these tabs are stored in Active Directory/ADAM and are replicated (this is configurable) to the client systems.

Alternatively, System Policy settings applied on the server can be viewed and modified locally on the client systems, only if:

- the **Client Configuration** option was selected at install time, or
- the **ERA_CLIENT_CONFIGURATION_ONLY** property in the **SafeNet ProtectDrive.msi** was set to configure the client locally via the Local Management Console.

© SafeNet, Inc.

Sample Configuration

The following steps outline how to configure a client system.

1. On the server, open the **ProtectDrive Management Console**.

2. Open the **Active Directory Users and Computers** MMC snap-in, right-click on the client PC's name, and then select **Properties**.

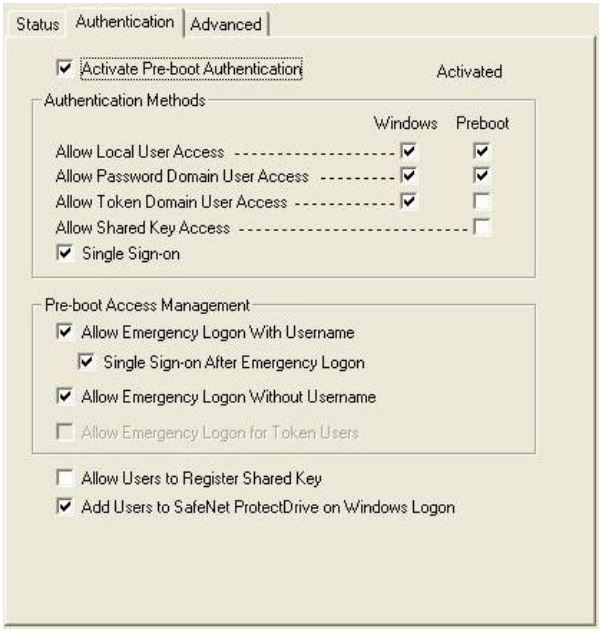
   -OR-

   Open the **ProtectDrive Management** snap-in, select **Configuration Objects**, right-click on **ProtectDrive Default Configuration** or alternative configuration object (to which the client had been, or will be assigned), and then select **Properties**.

3. Click the **PD Settings** tab and use all the displayed tabs to set the desired ProtectDrive System Policy.

4. Go through all the ProtectDrive tabs and set the client PC's System Policy accordingly. Pay particular attention to the settings outlined below.

   Authentication Tab



   - Click **Apply**, and then click **OK** to store System and User Policy data in Active Directory/ADAM and is time stamped in preparation for eventual replication to the client system(s). Replication of the configuration changes to the client(s) will take place in accordance with the update settings located in the **Management** group.

- Pay attention to the **Activated/Pending/Deactivated Indicator**. An example is shown below. The indicator shows the current status of the client's ProtectDrive Pre-boot Authentication. The ProtectDrive client **Activated/Deactivated** state gets updated in accordance with the settings in the **Management** group.

  When the setting of the **Activate Pre-boot Authentication** option changes, the ProtectDrive client goes through a delayed transitionary period (indicated by **Pending**) before the actual **Activated** or **Deactivated** state takes effect.

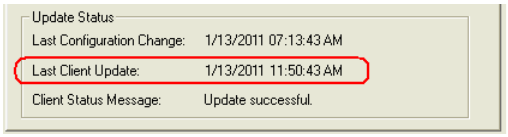
  In the above example, the indicator tells us that although the pre-boot authentication is activated (the check box is selected) no pre-boot users have replicated to the client—**yet**. Therefore, for the time being, all ProtectDrive features are disabled on the system. This may be the case when ProtectDrive is first installed on the system, and the System Policy has not yet propagated to it from Active Directory/ADAM.

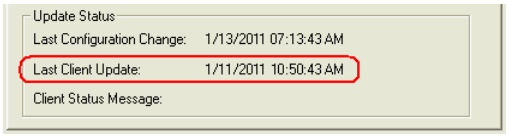
  Alternatively, the same effect will be achieved if no users have been assigned to the system. In short, the **Pending** status will prevail until the system is properly configured and the policy data successfully replicates from the server.

  If the **Activate Pre-boot Authentication** option is **reactivated,** ProtectDrive resets all user passwords to the configured initial pre-boot password, which may be explicitly defined in **PD Settings > Advanced > Password Policy**, where the default password is set to be equal to the username, or set to a designated default (the pre-set default is "*password*").

Status Tab

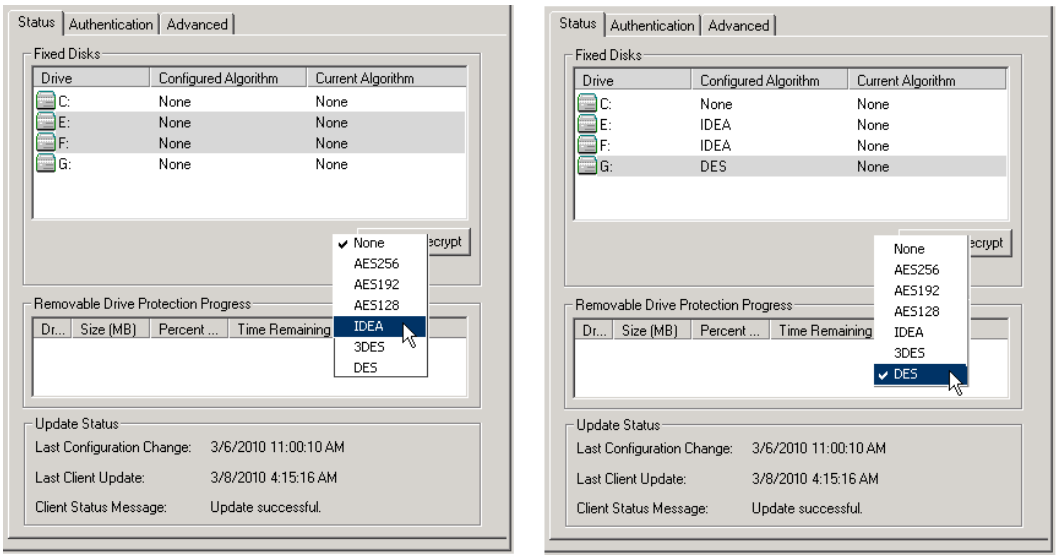
- Monitor the **Update Status** section on this tab for indication of the time of the most recent policy data change and client update. If the **Last Client Update** is chronologically later than the **Last Configuration Change**, then the policy data has successfully replicated to the client. In the following example, policy data has been successfully updated from the server (snapshot on the left). In the snapshot on the right, the client is still awaiting the next update.


Update Status
Last Configuration Change: 1/13/2011 07:13:43 AM
Last Client Update: 1/13/2011 11:50:43 AM
Client Status Message: Update successful.

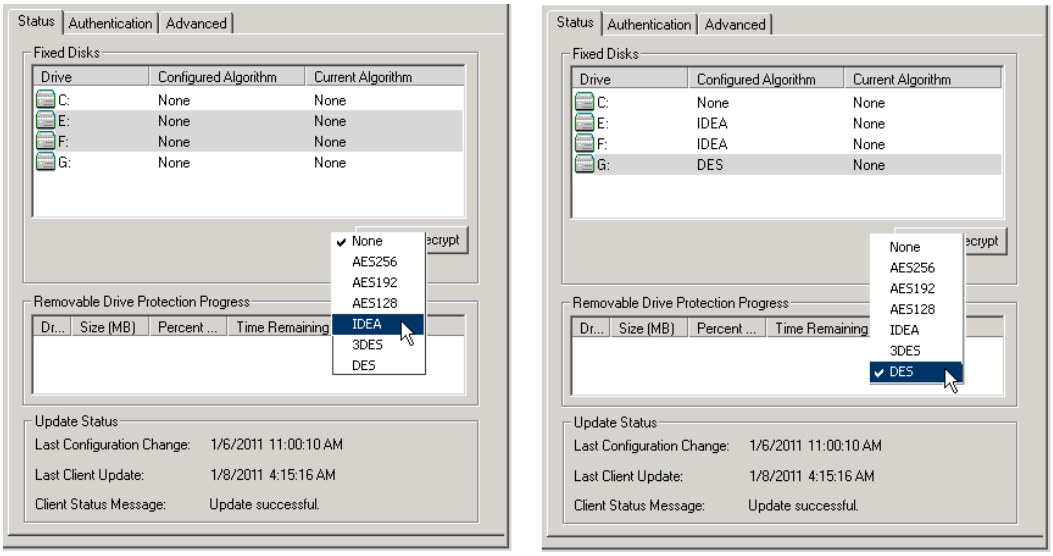

Update Status
Last Configuration Change: 1/13/2011 07:13:43 AM
Last Client Update: 1/11/2011 10:50:43 AM
Client Status Message:

© SafeNet, Inc.

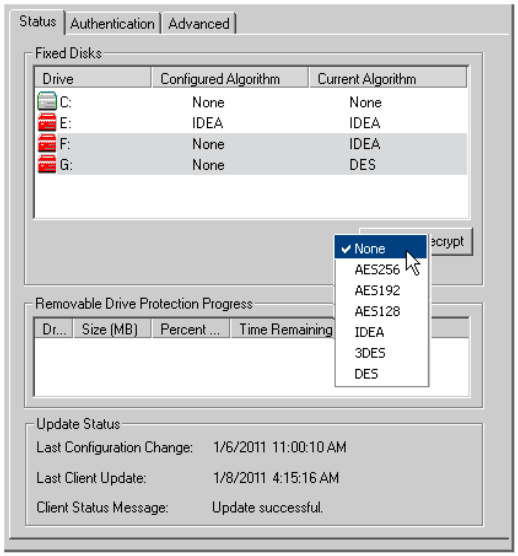
- Click the **Encrypt/Decrypt** button to specify which partitions on the client will be encrypted.



- Ongoing encryption progress will be indicated in half-shaded disk drive icons as follows (drive F on the left and drive G on the right).



- If you wish to decrypt any of the encrypted partitions, set the **Configured Algorithm** to **None**. In the following example, drives E and F are configured for decryption, which will take place as soon as the policy data replicates to the client in accordance with the **Updates** settings in the **Client Configuration** group**.**



© SafeNet, Inc.

Manage User Policy From the Server

Assigning Users to Clients and Managing User Policy via the Computer Object

Before configuring User Policy, review the contents of Chapter 7 – Configuring Default System and User Policy. This will familiarize you with the fields contained in the **PD Users** tab. This tab is used to configure ProtectDrive User Policy.

Sample Configuration

The following steps outline how to configure a client system.

1. On the server, open the **ProtectDrive Management Console**.

2. Open the **Active Directory Users and Computers** MMC snap-in, right-click on the client PC's name, and then select **Properties**.

   -OR-

   Open the **ProtectDrive Management** snap-in, select **Configuration Objects**, right-click on **ProtectDrive Default Configuration** or alternative configuration object (to which the client had been, or will be assigned), and then select **Properties**.

3. Select the **PD Users** tab, and then add all of the Windows Domain users and user groups you would like to give pre-boot access to this on client system. For each user or group, click **Set** to set their device access permissions.

   Note that changes to device access permissions for any user or user group apply across the entire Windows Domain. Changing permissions here will make the change for all client systems where this user or group is listed.

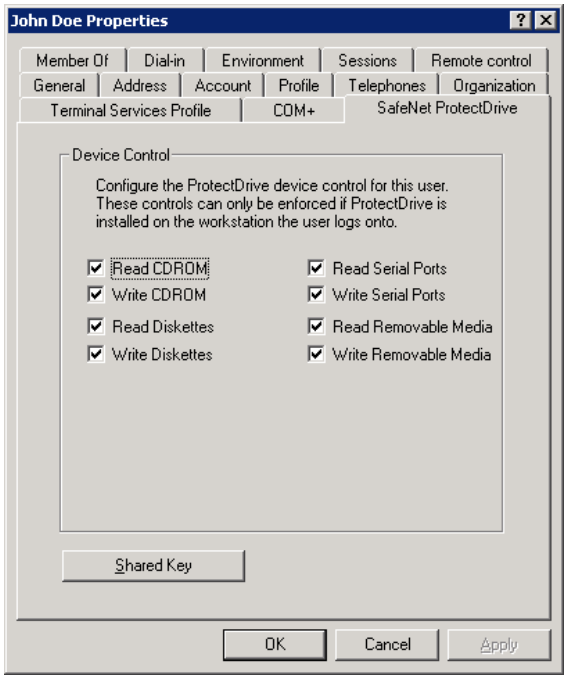
4. Select the **Certificate users also have password accounts** check box if you want to allow all users listed here pre-boot access with the use of the password, as defined by the **Default Password** in the **PD Settings > Advanced > Password Policy** group.

Managing User Policy via the User Object or Group Object

Set ProtectDrive device access permissions for individual Windows Domain users or user groups through either of the **ProtectDrive Management Console** snap-ins.

Use the Active Directory Users and Computers Snap-in (for Computer Object-managed Clients)

1. On the server, open the **ProtectDrive Management Console**.
2. Open the **Active Directory Users and Computers** MMC snap-in.
3. Open the **Users** directory.
4. Right-click on a Windows Domain user or user group name, and then select **Properties**.
5. Click the **SafeNet ProtectDrive** tab.
6. Set the device access permissions as appropriate for the user or user group.
7. Click **Apply**, and then click **OK**. These settings will be applied across the entire Windows Domain and will be picked up by all clients where this Windows Domain user or user group is listed.

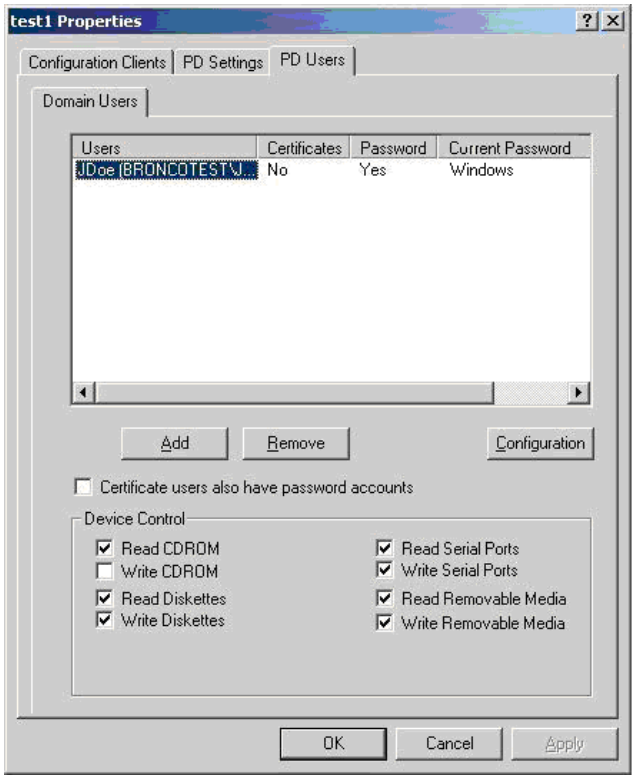


Settings that differ for various members of a user group will be grayed out, indicating conflicting data. Check these settings and set as appropriate.

© SafeNet, Inc.

Use the ProtectDrive Management Snap-in (for Configuration Object-managed Clients)

1. On the server, open the **ProtectDrive Management Console**.
2. Open the **ProtectDrive Management** snap-in.
3. Open the **Configuration Objects** directory.
4. Right-click on a configuration object, and then select **Properties**.
5. Click the **PD Users** tab, and then click on a user or user group name.
6. Set the device access permissions as appropriate for the user or group of users.
7. Click **Apply**, and then click **OK**. These settings will be applied across the entire Windows Domain and will be picked up by all clients where this Windows Domain user or group of users is listed.

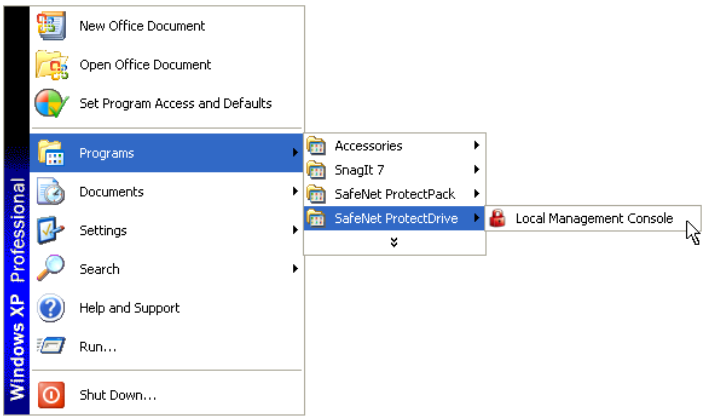


Settings that differ for various members of a user group will be grayed out, which indicates conflicting data. Check these settings and set as appropriate.

Manage System and User Policy Locally

The **Local Management Console** (LMC) utility is used to configure System and User policy locally or to view the configuration that was set by the ProtectDrive server. The tabs are very similar to the ones in the server's **ProtectDrive Management Console** (in the **Active Directory Users and Computers** MMC and **ProtectDrive Management** snap-ins). A few minor differences on the **PD Settings > Status** tab are described below.

To run the LMC utility from the Windows desktop, select **Start > Programs > SafeNet ProtectDrive > Local Management Console**.



You can also right-click on the ProtectDrive icon in the notification area, and then select **Local Management Console,** or simply double-click on the icon.

PD Settings Tabs

The **PD Settings** tabs are virtually the same in the LMC as they are in the server's **ProtectDrive Management Console** snap-ins.

The only exception is the **Status** tab, which, in the LMC, has three additional columns—**Size (MB)**, **Percent Encrypted**, and **Time Remaining**, described below. Refer to page 127 for a complete description of the **Status** tab.

Size (MB)

This column indicates the size of the hard drive partition.

Percent Encrypted

This column indicates the encryption status of the hard drive partition.

Time Remaining

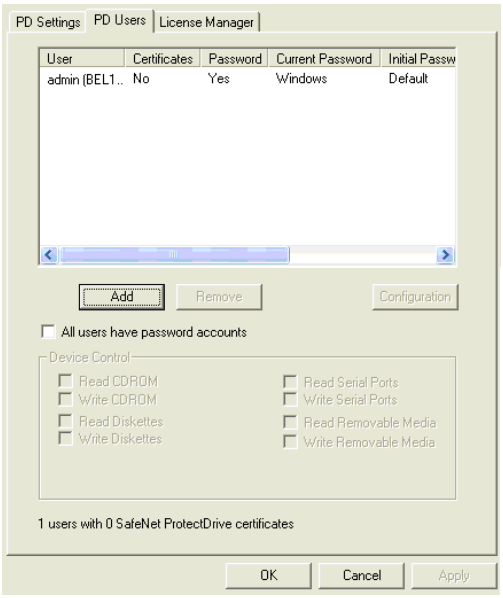
This column indicates the time remaining to completion while encryption is in progress.

© SafeNet, Inc.

PD Users Tab

Use the **PD Users** tab to add Windows Domain users and groups to the client. Note that all existing pre-boot user accounts are listed here.

Click **Add** to add Windows Domain users.



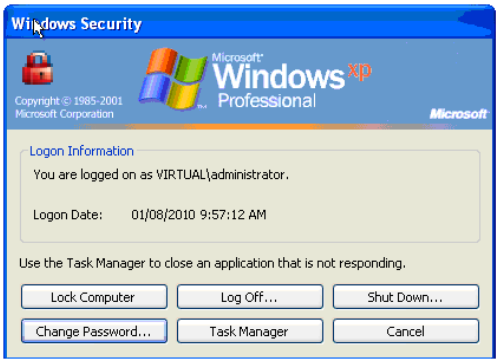
Add Local Windows Users to the ProtectDrive Pre-boot User Database

The easiest way to add local Windows users to the ProtectDrive Pre-boot user database is described below. Before you begin, go to the **PD Settings > Authentication** tab and verify the **Add Users to SafeNet ProtectDrive on Windows Logon** option is selected.

1. Log out of your Windows Administrator session on the client PC.
2. Have each user log into the local Windows. Once they successfully log in, their pre-boot user accounts will be automatically created.
3. Open the **PD Users** tab and verify each user has been added.

Change a Pre-boot Password

1. Press **CTRL-ALT-DEL** and select **Change Password**.



2. Verify the appropriate domain is selected in the **Log on to** field.

3. Specify the old and new password, and then click **OK**.

ProtectDrive will automatically synchronize passwords during a password change.

© SafeNet, Inc.

Chapter 9
User Authentication

If System policy has been configured to disable pre-boot authentication (see **Activate Pre-boot Authentication** in the **Authentication** tab), then none of the material in this chapter applies. In this case, the user will be presented with a standard Windows Domain authentication dialog, and normal Windows logon applies.

The default (high resolution) pre-boot screens shown in the following examples have a black background. If high resolution is not supported, then the pre-boot screens have a white background, which is typical of the *legacy* pre-boot screens. These low resolution screens function virtually the same as their high resolution counterparts.

Please note the following:

- Legacy pre-boot screens do not support fingerprint logon.
- Legacy pre-boot screens do not support auditory prompting.
- If both the **Allow Password Domain User Access** and the **Allow Token User Domain Access** pre-boot authentication options are enabled in ProtectDrive, the legacy screens do not include an initial pre-boot screen (shown in the example below), which allows the user to choose the login method. Instead, the user must press the **[F2]** function key to toggle between these two logon screens. If a PIN-only login is required, then this login selection screen does not display.

Default Initial Pre-boot Screen—choose login method

- In the case of consecutive failed pre-boot authentication attempts, the Lockout configuration policy will be enforced to prevent PIN guessing. (Open the system's **Event Viewer** for details on failed logon attempts and other events. See page 184 for more on **Event Viewer**.)

Authenticate with Smart Card/Token and PIN/Fingerprint

Pre-boot Authentication

Refer to Appendix A for a detailed diagram of the Smart Card/Token and PIN/Fingerprint Pre-boot Authentication logic flow.

If the ProtectDrive **Allow Token Domain User Access** or **Allow Shared Key Access** Authentication option is set, then the pre-boot authentication screen will be as shown below.

Default Smart Card/Token and PIN Log On Screen

Legacy Smart Card/Token and PIN Log On Screen

(High resolution only) If smart card/token log in requires a fingerprint, the inserted smart card or token is fingerprint-enabled, *and* a biometric reader is detected, then the pre-boot authentication screen will display as shown below. PIN entry is an alternative logon method on this screen. (Cards used for fingerprint logon must be initialized as PKI cards with BSEC middleware version 7.1.1 or higher.)

Default Smart Card/Token and PIN/Fingerprint Log On Screen

After selecting a finger to be read from the **FINGER** drop-down list, the user will then be prompted to position a finger on the biometric reader to complete the logon process.

Single sign-on is currently not supported with biometric (fingerprint) logon. The user will be required to log into Windows after logging in to ProtectDrive. Refer to *Windows Authentication* starting on page 149.

© SafeNet, Inc.

Windows Authentication

Every time a user successfully logs into Windows, their most current Windows Password propagates to the ProtectDrive Pre-boot User database.

Refer to Appendix C for a detailed diagram of the Windows (Domain) authentication logic flow.

Automatic - Single Sign-on Mode is ON

Assuming the ProtectDrive Single Sign-on mode is ON, the user is automatically authenticated into their relevant Windows Domain.

Single sign-on is currently not supported with fingerprint logon.

Manual - Single Sign-on Mode is OFF

In the case of no Single Sign-on, the standard Windows Domain authentication screen will display (if fingerprint authentication is not used), similar to the one shown below.

If fingerprint authentication is used, refer to *Manual – Fingerprint Authentication* on the next page.

Inserting the smart card/token into the reader will result in the standard Windows Domain PIN authentication screen, similar to the one shown below. At this point, the user enters their PIN.

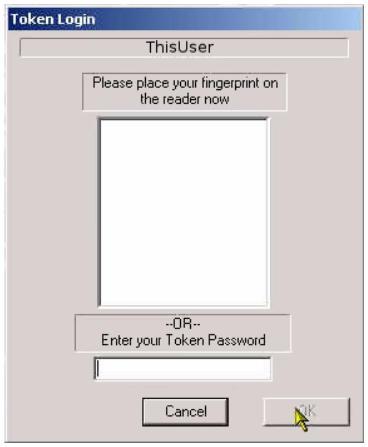
Alternatively, assuming that either the **Allow Local User Access** or the **Allow Password Domain User Access** option is set (on the **Authentication** tab), the user may press **Ctrl-Alt-Del** to invoke the standard Windows Domain Log On screen (see page 152).

Manual - Fingerprint Authentication (Single Sign-on Mode is not supported)

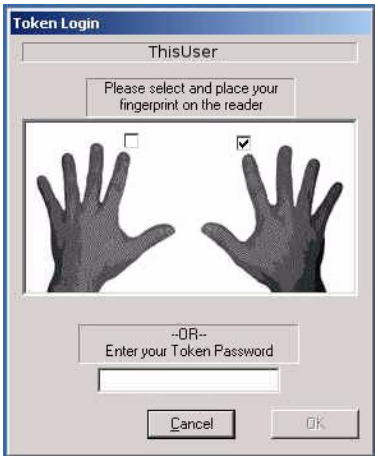
Single Sign-on is currently not supported with fingerprint logon. This means you are not automatically logged into Windows after you've successfully logged into ProtectDrive.

After logging in to ProtectDrive, you are immediately presented with a *Token Login* screen (shown below), rather than the Windows *Log On* screen as shown in the previous examples. On the *Token Login* screen, you can use either fingerprint authentication, or log in with a PIN.

If a fingerprint is used, note that the system can be configured to accept up to four fingerprints. The number of fingerprints that are ~~"e~~nrolled" will determine the login screen that displays. Refer to the *SafeNet Borderless Security PK and SSO User Guide* for details on fingerprint enrollment.



One fingerprint enrolled



More than one fingerprint enrolled

After authentication is successful, the Windows desktop displays.

Token Removal Policy

Computers using tokens or smart cards for Windows Domain authentication can be configured to automatically lock the system when the token is removed.

This behavior is controlled by the **Smart card removal behavior** policy in the **MMC Local Security Settings** snap-in. By default, this policy is set to **No action** or **Not defined**.

SafeNet recommends setting this policy to **Lock Workstation**. This setting will require the user to re-insert their token and enter their PIN upon returning to the workstation.

© SafeNet, Inc.

Authenticate with Username, Password, and Domain Name

Pre-boot Authentication

Refer to Appendix B for a detailed diagram of the Username/Password/Domain Name pre-boot authentication logic flow.

If either the **Allow Local User Access** or the **Allow Password Domain User Access** option (on the **Authentication** tab) is set, the following ProtectDrive pre-boot authentication screen will display.

Default Username/Password/Domain Log On Screen

Legacy Username/Password/Domain Log On Screen

The **Domain** field lists all the relevant Windows Domains available on the system. Use the **[Up-Arrow]** and **[Down-Arrow]** to navigate the list of available domain names.

Assuming the **Allow Local User Access** option (on the **Authentication** tab) is selected, the *Local System Name* will also be listed in the **Domain** field of the following ProtectDrive pre-boot authentication screen.

Note that in the case of consecutive failed pre-boot authentication attempts, the lockout policy will be enforced to prevent password guessing. (Open the system's **Event Viewer** for details on failed logon attempts and other events. See page 184 for more on **Event Viewer**.)

Windows Authentication

Every time a user successfully logs into Windows, their most current Windows Password propagates to the ProtectDrive Pre-boot User database.

Automatic - Single Sign-on Mode is ON

Assuming the ProtectDrive Single Sign-on mode is ON, the user is automatically authenticated into their relevant Windows Domain following successful pre-boot authentication.

Manual - Single Sign-on Mode is OFF

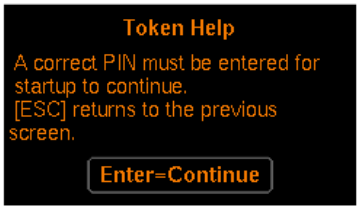
If Single Sign-on is not enabled, the following standard Windows Domain authentication screen will display:

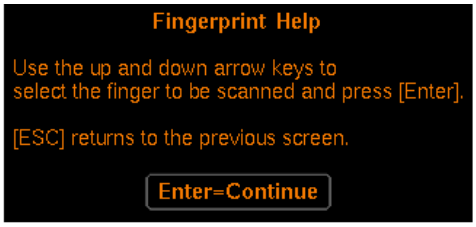
The following standard Windows Domain authentication screen will display after pressing **Ctrl-Alt-Del**. The relevant Windows Domain User Names and Passwords apply.

© SafeNet, Inc.

Helpful Hints

- (Legacy pre-boot screens only) If the system has been configured to allow *Smart Card/Token/PIN* access as well as *Username/Password/Domain Name*, press the **[F2]** function key to switch from one login method to the other.
- (Default pre-boot screens only) A blank screen saver will automatically take effect when a workstation is left unattended for at least 10 minutes.
- From either type of pre-boot login screen (**User Name/Password/Domain** or **PIN/Fingerprint**), press the **[Esc]** key to return to the previous screen.
- Press the **[F1]** function key to display **Help** from any pre-boot log on screen. A few examples are shown below.




Fingerprint Help
Use the up and down arrow keys to select the finger to be scanned and press [Enter].
[ESC] returns to the previous screen.
Enter=Continue

- In the case of consecutive failed pre-boot authentication attempts, the Lockout configuration policy will be enforced to prevent PIN guessing. (Open the system's **Event Viewer** for details on failed logon attempts and other events. See page 184 for more on **Event Viewer**.)

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Chapter 10
Extraordinary Authentication Scenarios

To retrieve a client's recovery envelope from Active Directory for password recovery, the client installation **MUST** be set to Remote Configuration from the Active Directory install. This will ensure that the client can be remotely configured via Active Directory.

To ensure Active Directory updates and envelope retrieval on the client, set the SafeNet ProtectDrive.msi **ERA_CLIENT_CONFIGURATION_ONLY** property to 0.

If an installation has **not** been installed as a Remote Configuration, this can be changed by setting the **ClientConfigurationOnly** DWORD value registry setting to 0 in *HKLM/Software/SafeNet/ProtectDrive/Installer*, and then rebooting the computer. The recovery envelope will not be available from Active Directory with this method, but it will still be available from the .env file created at install.

If System Policy has been configured to disable pre-boot authentication (see the **Activate Pre-boot Authentication** option on the **Authentication** tab), then none of the material in this chapter applies. In this case, the user is presented with a standard Windows Domain authentication dialog, and normal Windows logon applies. In addition to normal pre-boot user authentication, System Policy can be configured to accommodate the following extraordinary circumstances:

- Emergency Logon for Token Users Procedure – This procedure is used when a token user misplaces their smart card/token or forgets their PIN. This procedure allows for one-time pre-boot access to the system with assistance from the System Administrator. Note that emergency login for a token user will not be able to be performed until the token user logs in (after this selection has been made).

- Emergency Logon With Username Procedure – This procedure is used to accommodate a Windows Domain or Local Windows user who has forgotten his/her Windows Password. Pre-boot access to the system can be achieved with some help from the System Administrator. Note that emergency login for a user will not be able to be performed until the user logs in (after this selection has been made).

- Emergency Logon Without Username Procedure –This procedure is used to accommodate an emergency logon for users who have forgotten their username, or for adding newly added Windows Domain or Local Windows users to the client system's Pre-boot User database.

  In addition, this procedure would be appropriate in situations where the Active Directory User Policy has not yet replicated to the client system prior to the user's initial pre-boot authentication. Once the user executes this procedure and then authenticates into Windows, an account is created for him/her in the local system's Pre-boot User database.

- Unattended Reboot with Automatic Pre-boot Authentication – If an unattended reboot, followed by an automatic pre-boot authentication, is needed by the System Administrator, then a special Pre-boot User account must be created. This function is **not** controlled by System Policy. Instead, the System Registry must be amended as described later in this chapter.

Emergency Logon for Token Users Procedure

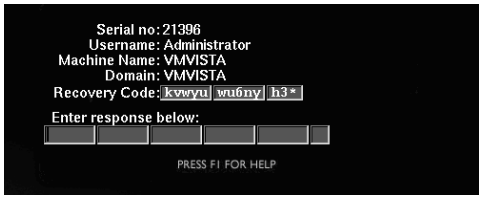
End-User Instruction

If a *Smart Card/Token/PIN/Fingerprint* user misplaces their smart card/token or forgets their PIN, access to the system may be achieved by performing the ProtectDrive *Emergency Logon for Token Users* procedure (at the discretion of the System Administrator):

1. Place the cursor in the **PIN** field and press **Shift+F9**.

or

The following recovery/response screen displays:



© SafeNet, Inc.

2. Contact your System Administrator (either in person or by phone) and communicate to them the displayed *Recovery Code (Challenge)*.

3. In return, the Administrator will communicate to you to the *Response Code*. Enter this code into the **Enter response below** field shown below.

4. At this point, Windows will proceed to load normally and will either log you on to Windows *automatically* or *manually*, depending on how the System Administrator configured ProtectDrive.

System Administrator Instruction

The user will perform the procedure on the previous page, and contact the System Administrator. In turn, the System Administrator will use the Recovery File Set (originally created after the ProtectDrive install) to perform the following steps to complete the emergency logon procedure.

1. Run **rpadmin.exe**, located in *\Program Files\SafeNet ProtectDrive* on the server. The ProtectDrive *Remote Recovery Console* window displays.

2. Click the **Emergency Logon** tab.

3. In the **Recovery Support Certificate Key** section, select the appropriate **Recovery Support Certificate Key** option:

   - **Personal Store**—If you select this option, you must have the user's private recovery key certificate copied from their Personal Store to your machine.

   - **PFX File**—If you select this option, click ..., and then browse to and open the user's private **PdRecovery.pfx** file. Enter the password. (Entering a password will enable the **Generate Response** button.)

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

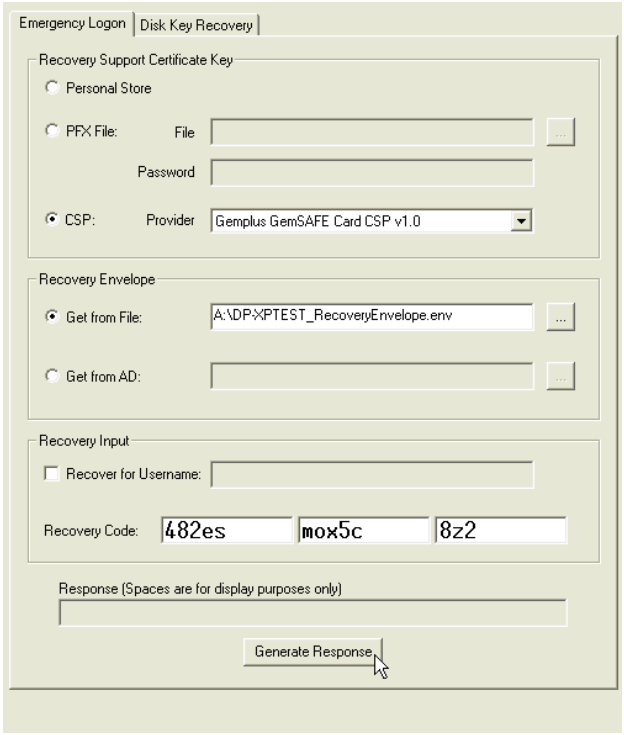
4. Select the **Recovery Envelope** file for the user's computer:

   - **Get From File**—If you select this option, click ..., and then browse to and open the **<computername>_RecoveryEnvelope.env** file.

   - **Get From AD**—If you select this option, click ..., and then browse to the Active Directory computer and locate the computer object.

     This option will only work if the client was installed as remotely configured with an Active Directory install.

5. Enter the code provided by the user into the **Recovery Code** field, and then click **Generate Response**.



6. Instruct the user to enter the automatically generated response code into the **Enter response below** field. At this point, the user will be granted pre-boot access to the system.

© SafeNet, Inc.

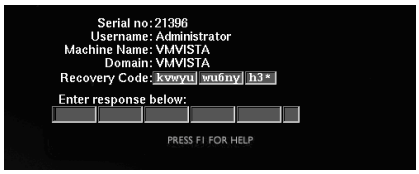
Emergency Logon With Username Procedure

End-User Instruction

If a *Username/Password/Domain Name* user forgets their password, the *Emergency Logon With Username* procedure can be used to gain access to the system.

1. Enter your username into the **User ID** field of the *Username/Password/Domain Name Log On* screen, shown below.

2. Place the cursor in the **Password** field and press **Shift+F10.** The following recovery/response screen displays.



3. Contact your System Administrator (either in person or on the phone) and communicate to them the displayed *Recovery Code* (*Challenge*) along with your *Username*.

4. In return, the Administrator will communicate to you the *Response Code.* Enter this code into the **Enter response below** field.

5. At this point, Windows will proceed to load normally and will either log you on to Windows *automatically* or *manually,* depending on how the System Administrator configured ProtectDrive.

System Administrator Instruction

The user will perform the procedure on the previous page, and contact the System Administrator. In turn, the System Administrator will use the Recovery File Set (originally created after the ProtectDrive install) to perform the following steps to complete the emergency logon procedure.

1. Run **rpadmin.exe**, located in *\Program Files\SafeNet ProtectDrive* on the server. The ProtectDrive *Remote Recovery Console* window displays.

2. Click the **Emergency Logon** tab.

3. In the **Recovery Support Certificate Key** section, select the appropriate **Recovery Support Certificate Key** option:

   - **Personal Store**—If you select this option, you must have the user's private recovery key certificate copied from their Personal Store to your machine.

   - **PFX File**—If you select this option, click , and then browse to and open the user's private **PdRecovery.pfx** file. Enter the password. (Entering a password will enable the **Generate Response** button.)

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

4. Select the **Recovery Envelope** file for the user's computer:

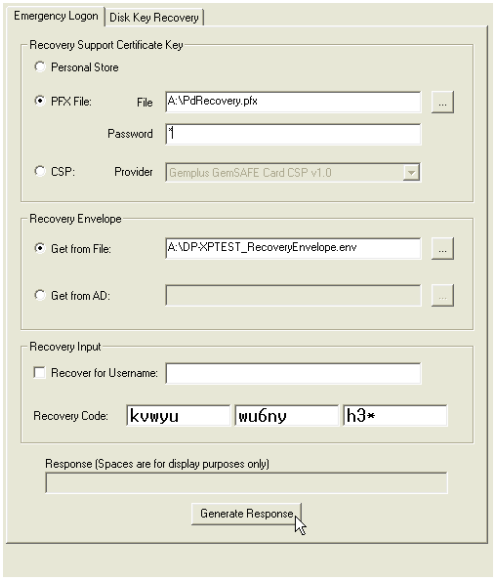
   - **Get From File**— If you select this option, click , and then browse to and open the **<computername>_RecoveryEnvelope.env** file.

   - **Get From AD**— If you select this option, click , and then browse to the Active Directory computer and locate the computer object.

     This option will only work if the client was installed as remotely configured with an Active Directory install.

© SafeNet, Inc.

5. Enter the code provided by the user into the **Recovery Code** field, and then click **Generate Response**.



6. Instruct the user to enter the automatically generated response code into the **Enter response below** field. At this point, the user will be granted pre-boot access to the system.

7. For security purposes, instruct the user to change their Windows (Domain) Password as soon as they log on to Windows.

Emergency Logon Without Username Procedure

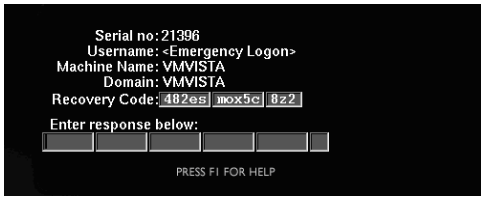
This procedure does **not** apply to the smart card/token and PIN users.

If a user has not yet had the opportunity to log on to their ProtectDrive secured PC, they may be required by the System Administrator to execute the following *Emergency Logon Without Username Procedure* during their first-time-ever system log on.

End-User Instruction

1. Place the cursor in the **User ID** field of the *Username/Password/Domain Name Log On* screen shown below and press **Shift+F9**.

   The following recovery/response screen displays.



2. Contact your System Administrator (either in person or phone) and communicate to them the displayed *Recovery Code (Challenge)*.

3. In return, the System Administrator will communicate to you the *Response Code*. Enter this code into the **Enter response below** field.

4. At this point, one-time-only pre-boot access to the system is granted. Proceed to normal Windows log-in.

© SafeNet, Inc.

System Administrator Instruction

The user will perform the procedure on the previous page, and contact the System Administrator. In turn, the System Administrator will use the Recovery File Set (originally created after the ProtectDrive install) to perform the following steps to complete the emergency logon procedure.

1. Run **rpadmin.exe**, located in *\Program Files\SafeNet ProtectDrive* on the server. The ProtectDrive *Remote Recovery Console* window displays.

2. Click the **Emergency Logon** tab.

3. In the **Recovery Support Certificate Key** section, select the appropriate **Recovery Support Certificate Key** option:

   - **Personal Store**—If you select this option, you must have the user's private recovery key certificate copied from their Personal Store to your machine.

   - **PFX File**—If you select this option, click , and then browse to and open the user's private **PdRecovery.pfx** file. Enter the password. (Entering a password will enable the **Generate Response** button.)

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

4. Select the **Recovery Envelope** file for the user's computer:

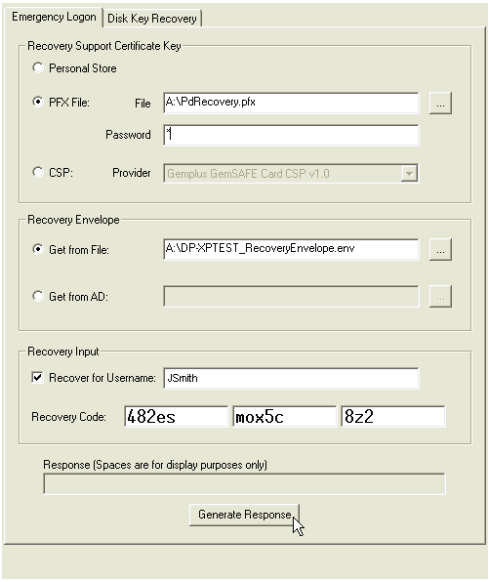
   - **Get From File**— If you select this option, click , and then browse to and open the **<computername>_RecoveryEnvelope.env** file.

   - **Get From AD**— If you select this option, click , and then browse to the Active Directory computer and locate the computer object.

     This option will only work if the client was installed as remotely configured with an Active Directory install.

5. Select the **Recover for Username** check box and enter the user's name.

6. Enter the code provided by the user into the **Recovery Code** field, and then click **Generate Response**.



7. Instruct the user to enter the automatically generated response code into the **Enter response below** field. At this point, the user will be granted one-time pre-boot access to the system.

   Once the user successfully completes their post-boot Windows authentication, a new pre-boot user account is created for them in the local system's ProtectDrive Pre-boot User database.

Unattended Reboot and Automatic Pre-boot (APB) Authentication

Certain system administration tasks require unattended system reboots and automatic loading of the operating system. For these purposes, ProtectDrive is provisioned for creation of the Dummy Pre-boot User account.

Creation of this account, combined with the following additions to the Windows Registry, allows for the automatic, unattended pre-boot system authentication. Note that the unattended pre-boot will disable Single Sign-On independent of the System Policy setting. The system will automatically log in at pre-boot, load Windows, and stop at the Windows (Domain) *Log On* screen.

© SafeNet, Inc.

The Unattended Pre-boot Authentication setup procedure is as follows:

1. Create a new pre-boot user account with **any unique** Username and Password. One way to do this is to use **pduserdb.exe** (see Chapter 11)**.**

2. Amend the Windows Registry as shown below:

   HKLM\Software\SafeNet\ProtectDrive

Refer to the table below for details on the key values you can add to this account.

After adding the keys for APB, every type of logon (for example, RDP connection, log off/log on, etc.) will cause the deletion of that specific key.

APB_COUNT	REG_DWORD **0,**N	Set to zero (0) by default, this option allows no automatic pre-boot authentication. If any of the automatic pre-boot authentications attempts fails, this value is reset back to zero (0). If set to a value greater than 0 (0<N<65535), then N number of automatic pre-boot authentications is allowed. Set to 0x0000FFFF or greater for unlimited automated pre-boot authentications.
APB_USERNAME	REG_SZ	Username
APB_PASSWORD	REG_SZ	User Pre-boot Password. Use this option to enter the PIN for the token if APB_TOKEN is used.
APB_DOMAIN	REG_SZ	Domain Name for the User
APB_RESETINTVECTS	REG_DWORD **0,**1	Set to zero (0) by default, this option causes no change in the normal ProtectDrive operation. When set to (1), this option will suppress the standard ProtectDrive warning message displayed when any system tampering is detected. This can be useful when performing a BIOS upgrade, which can change the interrupt vector addresses as part of automated system maintenance.
APB_TOKEN	REG_DWORD **0,**1	When set to (1), this option will ignore the APB_USERNAME and APB_DOMAIN entries, and will logon to the token using the PIN defined by the APB_PASSWORD option.
APB_PERSISTENCE_LEVEL	REG_DWORD **0,**1	Set to zero (0) to save the APB information on graceful shutdown or restart. This is effectively the same as no APB_PERSISTENCE_LEVEL entry at all. Set to (1) to save the APB information at Windows startup, as well as on graceful shutdown or restart. This setting, although not as secure, will still allow for APB after an unexpected shutdown or power failure.

Creating a Disaster Recovery Disk Key

This procedure is used to recover a hard disk in the event that a ProtectDrive-encrypted computer fails to boot to Windows.

In this procedure, the System Administrator will create a disk key file by using the **rpadmin** utility. The disk key file, encrypted with a passphrase, is used with the **decdisk** utility and the EFS recovery files (created with the **backup.exe** utility, or obtained from Active Directory at the same time as the disk key creation) to complete the disk decryption and recovery procedure.

Refer to Chapter 11 for details on backup.exe, decdisk.exe.

A recovery disk key is also required for the **peprep** utility (the WinPE bootable disk recovery utility). Refer to Chapter 11 for details on peprep.exe.

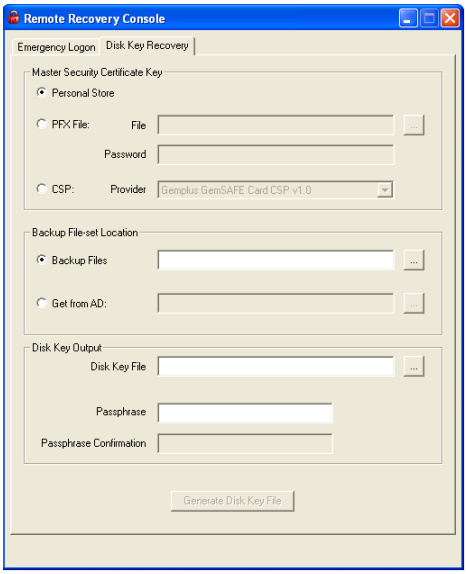
Create the Recovery Disk Key

This procedure must be performed by the System Administrator. Before you begin, make sure you have the following:

- **decdisk.exe** utility
- **EFS recovery files** from the system to be recovered (created with **backup.exe** or obtained from Active Directory)
- **Master Security Certificate** key (for example, the .pfx file)

1. Run **rpadmin.exe**, located in *\Program Files\SafeNet ProtectDrive* on the server. The ProtectDrive *Remote Recovery Console* window displays.

2. Click the **Disk Key Recovery** tab.



© SafeNet, Inc.

3. Select the appropriate **Master Security Certificate Key** option:

   - **Personal Store**—If you select this option, the Master Security Certificate's private key must be in the user's Personal Certificate Store on your machine.

   - **PFX File**—If you select this option, click ..., and then browse to the **PdMaster.pfx** file and enter the password.

   - **CSP**—If you select this option, choose the appropriate **Provider** from the drop-down list where the certificate key is stored.

4. Specify the **Backup File-set Location**:

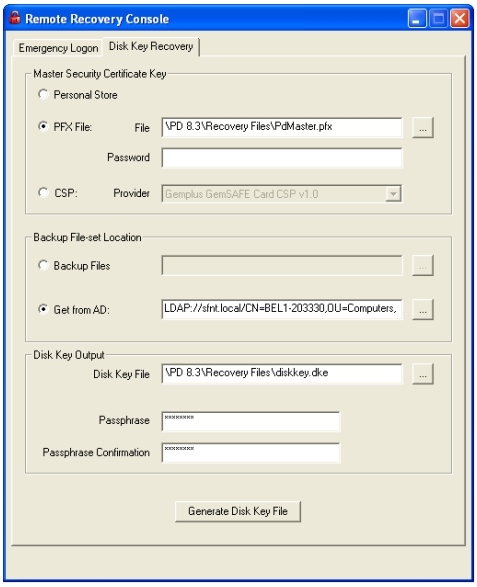
   - To locate the backup file set (created with the backup.exe recovery tool—see Chapter 11 for details), click the **Backup Files** option, click ..., and then browse to the folder location, and click **OK**.

   - To locate the backup file set on the Active Directory computer, click the **Get from AD** option, click ..., and then browse to the computer object in the domain where the backup file set is located, and click **OK**.

     The ACSVER, BACKUP. TLV, DKENV, DTE, GDA, and MBR recovery files will be saved to the same location as the disk key (.dke) file specified in the next step.

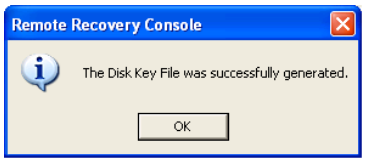
5. Enter the **Disk Key File** name (for example, **diskkey.dke**), click ... and then browse to the location where the file should be saved, and click **Save**.

6. Enter and confirm the passphrase for the key file. For your reference, a completed sample **Disk Key Recovery** screen is shown below.



7. Click **Generate Disk Key File**.

8. Click **OK** when the Disk Key File is successfully generated.



Recover (Decrypt) the Disk

Before you begin, verify that you have the **decdisk.exe** utility, the encrypted ***.dke** file and corresponding passphrase, and the EFS recovery files.

1. Boot the affected PC into DOS mode.

2. From the command line, decrypt the hard disk using the ProtectDrive **decdisk** utility. Make sure you use the **/dk** option.

   For example, **`decdisk -dk diskkey.dke`**

3. Enter the passphrase (created in step 6 in the previous section) when prompted.

4. Select the area of the disk to be decrypted when prompted.

5. After decrypting the disk, run **rmbr /o /r /rp** <backup-files-path> (to remove the ProtectDrive pre-boot authentication), and then reboot the PC.

   For details on the RMBR recovery utility, refer to page 178.

   If the system drive remains unbootable (which indicates it is heavily corrupted), try to regain a standard bootable MBR on it by using any system or third-party aid. The information on the following Web page may help you choose a system method of MBR repair: http://fixmbr.net/. Keep in mind that forcing the system drive to boot will not succeed if its decryption is not completed.

6. After the PC reboots, uninstall ProtectDrive.

7. Discard the encrypted ***.dke** file and passphrase, as they are now obsolete.

© SafeNet, Inc.

Chapter 11
RapidRecovery™ Disaster Recovery Tools

Introduction

This chapter details the utilities that SafeNet offers in its RapidRecovery™ suite of recovery tools. These command line utilities must be run by an administrator. With these tools, you will be able to safely recover a ProtectDrive system in as little as five minutes.

BACKUP.EXE – Creating ProtectDrive Recovery Files

In preparation for disaster recovery, the command prompt utility, **backup.exe**, must be used following each disk encryption status change or license update. A folder, labeled with the computer name, will be created with the EFS recovery files inside, which are necessary for disk recovery. Note that you can also run this utility as a scheduled administrative task.

`Usage: BACKUP.EXE [options]`

Options	Description	Default
`/? | -usage`	Displays usage help	
`/v | -ver`	Displays utility version	
`/t | -tgt`	Specifies target directory for backed up **Recovery Files**	Current directory. Note that it may be good practice to store the Recovery Files off the client system. This will ensure their availability in the rare case when the client system is rendered inoperable.
`/n | -noverchk`	No ProtectDrive version compatibility check is performed. For example, an 8.2.1 version of backup.exe can be run on an 8.5 version of ProtectDrive. If /n is not used, a message will display to notify the user that there is a version mismatch between the backup.exe and the ProtectDrive version.	

If, for some reason, the ProtectDrive secured system becomes inaccessible (due to data corruption, for example) the System Administrator can use the following disaster recovery tools to perform system diagnosis, decrypt the hard disk(s), manipulate the MBR, and administer the Pre-boot User database.

The following tools are included in the *\Tools* directory of the ProtectDrive distribution CD. These tools, along with the original **salt.cid** and the **EFS recovery files**, provide enough functionality to recover any inoperable ProtectDrive system.

DECDISK.EXE - Disk Decryption Utility

This 16-bit, MS-DOS command prompt disk decryption utility is only used to decrypt a *non-bootable Windows installation* (i.e., when access to the GUI-based decryption mechanism is not available). If Windows is bootable, use the decryption mechanism in the **ProtectDrive Management Console** snap-ins, in **PD Settings > Status**.

After a successful decryption using **decdisk**, and a successful Windows boot occurs, the disk is re-encrypted.

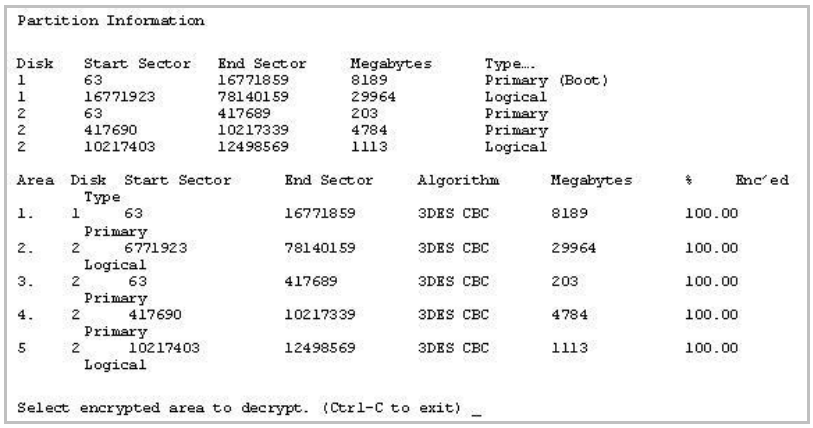
`Usage: DECDISK.EXE [options]`

Options	Description	Default
`/? | -usage`	Displays usage information	
`/v | -ver`	Displays utility version information	
`/d | -display`	Displays encryption information only	
`/a | -all`	Decrypts all encrypted partitions; not recommended for third-party disk recovery, as this option may decrypt the wrong disk	User specified
`/e | -est`	Estimates the region intended for decryption and forces the /r option	
`/r | -rec`	Uses *Recovery Files* for the decryption operation	
`/rp | -recpath`	Specifies the path to the *Recovery File* (points to the backup file set created with backup.exe)	Current directory
`/dk | -diskkeyfile`	This option must always be used. It specifies the encrypted diskkey file used for disk key recovery. Can be used in conjunction with the /r option. Allows the user to read the diskkey from the encrypted *.dke file.	
`/mbr | -restorembr`	Restores original MBR.	
`/s | -sel`	Selects the installation partition.	

© SafeNet, Inc.

Decdisk will initially display a Partition Information section for all known hard disks. The output will be similar to the example shown on the next page.

If you notice an incorrect disk number in the Encryption Information section in the **decdisk** output, exit **decdisk** and re-run it with the **/e** option to enter the correct information manually.



```
Partition Information

Disk    Start Sector    End Sector      Megabytes       Type...
1       63              16771859        8189            Primary (Boot)
1       16771923        78140159        29964           Logical
2       63              417689          203             Primary
2       417690          10217339        4784            Primary
2       10217403        12498569        1113            Logical

Area  Disk  Start Sector      End Sector      Algorithm       Megabytes       %     Enc'ed
      Type
1.    1     63                16771859        3DES CBC        8189            100.00
      Primary
2.    2     6771923           78140159        3DES CBC        29964           100.00
      Logical
3.    2     63                417689          3DES CBC        203             100.00
      Primary
4.    2     417690            10217339        3DES CBC        4784            100.00
      Primary
5     2     10217403          12498569        3DES CBC        1113            100.00
      Logical

Select encrypted area to decrypt. (Ctrl-C to exit) _
```

In the above example, **decdisk** displays information regarding all known hard disk partitions. **Disk** is the physical disk number. **Start Sector** and **End Sector** are relative to the start of the physical disk. **Decdisk** also displays information regarding the encryption status of the above partitions. The **Start Sector** and **End Sector** columns show the extent of the encryption. The value in the **Area** section is used to select which area to decrypt.

The information above portrays two physical disks. The first disk has primary and extended partitions containing one logical drive. The second disk contains two primary partitions and an extended partition containing one logical drive. All partitions on these disks are fully encrypted with Triple DES.

The user is required to select one of the encrypted areas to decrypt. As the decryption progresses, the user is informed of the percentage of the encrypted area still to be decrypted, and approximately how long the decryption will take as follows:

```
75.10%      3hrs:15mins remaining (Press Ctrl-C to stop)
```

Once the decryption is complete, the list of encrypted areas will be refreshed. When there are no more encrypted areas the following will message will display:

```
No encrypted areas found.
```

Using Recovery Files

If serious system corruption occurs, the ProtectDrive system files may not be accessible. In this case, **decdisk.exe** requires the backed up **Recovery Files**. These files are produced using **backup.exe** during normal ProtectDrive operation or obtained from Active Directory at the same time as disk key creation.

The following command line syntax example allows the user to select partitions for decryption:

```
decdisk -dk l:\pd\diskkeys\computer.dke -r -rp l:\pd\backups\computer\
```

where **l:\pd\diskkeys** is the path and **computer.dke** is the disk key file, and **l:\pd\backups\computer** is the path to the backup file set (i.e., the recovery file set).

After **decdisk** is run with the use of recovery files, it is necessary to run the **rmbr /o** command. After the PC reboots, uninstall ProtectDrive. Refer to *Recover the Disk* on page 168 for additional details.

Manually Specifying the Decryption Area

Decdisk decrypts disk areas selectable by sector number (using the **/e | -est** option). The user manually provides the **Start** and **End Sectors** and the **Algorithm** as follows:

```
Partition Information
Disk    Start Sector   End Sector     Megabytes      Type....
1       63             16771859       8189           Primary (Boot)

Enter disk number 1
Enter start sector 63
Enter end sector 16771859
Enter Alg (1=DES, 2 = 3DES, 3 = Idea) 3

----------------------
Area Disk Start Sector   End Sector    Algorithm     Megabytes % Enc'ed
1.    1     63            16771859     3DES CBC      8189       100.00

Select encrypted area to decrypt. (Ctrl-C to exit)
```


© SafeNet, Inc.

DISPEFS.EXE – ProtectDrive Diagnostic Utility

This diagnostic tool displays contents of the ProtectDrive system files. ProtectDrive stores system data in a number of files contained in the Embedded File System (EFS).

Usage: **DISPEFS.EXE [options] [>output_text_file]**

Options	Description
/? | -usage	Displays usage help
/v | -ver	Displays version information
/a | -all	Displays contents of all ProtectDrive system files
/d | -dtes	Displays drive table entries
/c | -cfg	Displays configuration data
/g | -gda	Displays general data
/x | -ex	Displays exchange data
/u | -user	Displays the Pre-boot User database.
/r | -rec	Displays data from *Recovery Files*
/rp | -recpath	Specifies the path to the *Recovery Files*
No Arguments	Displays all system files

PDUSERDB.EXE – Pre-boot User Database Administration Utility

This command line MS_DOS tool manipulates the ProtectDrive pre-boot user database, allowing the ProtectDrive Administrator to:

- List the names of users authorized to perform ProtectDrive pre-boot authentication.
- Remove Local and Domain (including Token/PIN user account) user accounts from the ProtectDrive pre-boot user database.
- Add Local and Domain user accounts (including Token/PIN user accounts) to the ProtectDrive user database.

`Usage:` **`PDUSERDB.EXE [options]`**

Options	Description
`/? | -usage`	Displays usage help
`/a | -add`	Adds a user to the pre-boot database
`/d | -domain`	Specifies the Windows Domain that the newly added user is a member of (defaults to the *Local System Name*). This domain name must be a NetBIOS domain name.
`/f | -file`	Specifies the filename of a file containing a user certificate
`/l | -list`	Displays a list of all existing pre-boot users
`/n | -name`	Specifies a username to add to the pre-boot database
`/p | -password`	Specifies the password of the newly added user
`/r | -remove`	Removes a user from pre-boot database
`/v | -version`	Displays version information

To change a password, remove the user account (/r) first, and then add a new account (/a) with the new password.

© SafeNet, Inc.

PEPREP.EXE – WinPE Bootable Recovery Disk Utility

WinPE (Windows Pre-Installation Environment) is a lightweight version of the Windows operating system, which can be used to run 32-bit or 64-bit recovery tools.

The **PEPREP** utility is a WinPE-based, pre-boot recovery tool, located in the *\Tools\WinPE* folder on the SafeNet ProtectDrive installation medium. It should be used by WinPE-savvy system administrators only.

PEPREP enables an authorized user (such as a Help Desk representative) to boot from a WinPE recovery disk (such as a USB drive or CD/DVD configured for WinPE) to a machine with ProtectDrive installed, and allows transparent encryption/decryption from the encrypted drive. During the recovery process, PEPREP copies files into a WinPE image before the image is ―bilt," and injects the appropriate disk key when WinPE is running.

Sample Scenario

A user's encrypted laptop or PC can no longer boot (through no fault of ProtectDrive), and she needs immediate access to critical files, PEPREP can assist an authorized Help Desk representative to recover the individual files within 30 minutes. Once recovered, these files can be copied over to a functional machine, and the end user can quickly resume her work.

Later, as time allows, the Help Desk representative can take the time needed to recover the entire laptop or PC.

Currently, ProtectDrive's WinPE support is intended only for systems with a *functional* ProtectDrive installation. If ProtectDrive files are corrupted, then PEPREP will not correct the problem.

Create the WinPE Bootable Recovery Disk

The following steps create a basic WinPE bootable ISO image. For more information on creating a WinPE image, go to http://technet.microsoft.com/en-us/default.aspx.

1. Download and install Microsoft's Windows Automated Installation Kit (WAIK). This can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&DisplayLang=en.

2. Open a Windows PE Tools Command Prompt from the Windows Start menu. Select ***Start\Programs\Microsoft Windows AIK***.

3. Create a Windows PE customization working directory. Run this command: ***copype.cmd winpe_x86 c:\temp\winpe_x86***

4. Expand the image for customization. Run this command:
   imagex /apply c:\winpe_x86\winpe.wim 1 C:\winpe_x86\mount

5. Configure the image for SafeNet ProtectDrive. Run this command:
   e:\tools\winpe\peprep /prep /img c:\winpe_x86\mount /pd e:\tools\winpe

   (where *e:* refers to the location of the SafeNet ProtectDrive installation files)

6. Copy the DKE file onto the image. Run this command:
   copy f: \targetcomputers.dke "c:\winpe_x86\mount\safenet protectdrive"

   The DKE files are created by running **rpadmin.exe**. A DKE file contains the encoded disk key. Refer to *Creating a Disaster Recovery Disk Key* on page 166 for details. Multiple DKE files can be copied onto the image if required.

7. Install the network card driver. The simplest method of copying files off the target computer is to use ***net use*** command to map a drive to other networked computers (see *Map a Network Drive* on page 177). If the target computer's network card is not supported by the operating system, you will need to install drivers for the device onto the image. For example:
   peimg /inf=<path to NIC Driver INF file> c:\winpe_x86\mount\Windows

8. Optimize the WinPE image for size. Run this command:
   peimg /prep /image=c:\winpe_x86\mount

   When prompted, enter ***yes*** to continue.

9. Capture the WinPE image. Run this command:
   imagex /capture /boot /compress max "c:\winpe_x86\mount" "c:\winpe_x86\iso\sources\boot.wim" "My PE Image"

10. Create the ISO image. The image, which now contains ProtectDrive support files, needs to be compressed back into the ISO form, which can then be burned to a CD or DVD. Run this command:
    oscdimg -n c:\winepe_sx86\iso c:\winpe_x86\my_pe_image.iso -n -bc:\winpe_x86\etfsboot.com

Inject the ProtectDrive Disk Key

Once the WinPE image has booted the affected computer, the disk key can be injected into the driver. You must know the .DKE file's password to complete this task.

1. Boot the affected computer from the WinPE recovery CD/DVD or USB drive.

2. Change the directory to *X:\Safenet ProtectDrive* and run
   peprep.exe –inj dsk.dke <enter>.

   Refer to the *PEPREP Command Line Options* section (below) for additional details.

© SafeNet, Inc.

3. When prompted, enter the DKE file's password.

4. After the disk key is verified, encrypted drives will now be accessible to recover the desired files.

Map a Network Drive

Once the network is connected, it is possible to access another computer on the same network. For example:

net use z: \\192.168.0.30\apps /user:mydomain\jdoe <enter>

You will be prompted for the user's password and once it is verified, files can now be copied from the target computer to the specified computer.

PEPREP Command Line Options

Usage: **PEPREP.EXE [options]**

```
peprep [/?] | [/v] | [/prep /img path /pd path] | [/inj file] | [/clean /img path]
```

Options	Description
/? | -usage	Displays usage help
/clean | -clean	Removes ProtectDrive WinPE support from an image
/e | -est	Estimates the region intended for decryption and forces the /r option
/img | -peimage	Path to the WinPE image (for example, *c:\winpe_x86\mount*)
/inj | -inject	Inject the disk key file (*.dke)
/pd | -pdfiles	Path to ProtectDrive WinPE support files
/prep | -prep	Prepare a WinPE image
/r | -rec	Uses *Recovery Files* for the decryption operation
/rp | -recpath	Specifies the path to the *Recovery File* (points to the backup file set created with backup.exe)
/u | -usb	Provides the ability to access USB drives
/v | -ver	Displays version information

RMBR.EXE – MBR Recovery Utility

The ProtectDrive Boot Manager/Master Boot Loader is the very first utility that runs after the system BIOS is loaded. ProtectDrive modifies part of the MBR during installation. This is done to enable ProtectDrive to locate its embedded file system upon system boot and prior to all other disk access. If the MBR is altered, replaced, or corrupted after the ProtectDrive install, the **rmbr.exe** utility is used to recover it.

Restoring the ProtectDrive MBR requires a sector-by-sector search of the embedded file system (EFS) located on the boot partition. Once the EFS is located, the ProtectDrive MBR can be restored.

`Usage:` **`RMBR.EXE [options]`**

Options	Description
`/? | -usage`	Displays usage help.
`/v | -ver`	Displays utility version.
`/p | -pd`	Recover the ProtectDrive MBR.
`/o | -original`	Recover the original (prior to the ProtectDrive install) system MBR.
`/r | -recovery`	Use the ProtectDrive Recovery Files to perform any of the above operations.
`/rp | -recpath`	Specifies the path to the *Recovery File* (points to the backup file set created with backup.exe or obtained from Active Directory).
`/s | -sel`	Selects the installation partition.

If the backup file set was provided during disk decryption (using **decdisk**) by invoking the "/r [/rp ..]" argument, then the same argument ("/r [/rp ..]") should be invoked with **rmbr** when restoring MBR.

RMBR Initial Status Check

Prior to performing any MBR recovery, **rmbr** will display the current MBR status. If the ProtectDrive MBR has been unaltered since the install, the following message displays:

```
Current MBR is the ProtectDrive MBR
```

However, if **rmbr** detects any alteration to the ProtectDrive MBR, the following message displays:

```
Current MBR is not the ProtectDrive MBR
```


© SafeNet, Inc.

RMBR Version Compatibility Check

Rmbr will attempt to verify that it is working with the correct version of the ProtectDrive system.

If the version is incorrect, the following message displays:

```
Incompatible versions
ProtectDrive Version: 8.1 (example)
RMBR.EXE Version: X.X.X (example)
```

Depending on the level of system data corruption, it is not always possible to determine the version of the currently installed ProtectDrive system.

Restoring the ProtectDrive MBR (RMBR /p)

RMBR will initially display the list of all ProtectDrive partitions. Select the partition you wish to recover the ProtectDrive MBR for.

```
Disk    Start Sector    End Sector      Megabytes       Type….
1       63              16771859        8189            Primary (Boot)
(ProtectDrive)

Select partition to recovery. (Ctrl-C to exit) _
Current MBR is not the ProtectDrive MBR
Searching for super block from sector 63 to sector 20487599
99.99% and 3hrs 20mins remaining. (Press Ctrl C to stop)
```

Rmbr.exe will search the disk sector by sector looking for the ProtectDrive super-block corresponding to the start of the ProtectDrive embedded file system. It is possible that remnants of previously installed ProtectDrive systems may exist on the disk. If a super-block is found, but it does not correspond to the current ProtectDrive installation, the following message displays:

```
Found super block at sector 1893443
Incorrect super block. Continuing search ..
```

If a valid super block is located, RMBR will display the version and ask the user for verification, as shown below.

```
Found super block at sector 1893443
ProtectDrive v8.1
Is this the correct version of ProtectDrive? [Y/N]
```

If the version is not correct, enter **N** and **rmbr** will continue. If the version is correct, enter **Y** and the following displays:

```
ProtectDrive MBR restored.
Current MBR is the ProtectDrive MBR.
```

Restoring the Original MBR `(RMBR /o)`

This option replaces the current MBR with the original system MBR that ProtectDrive saved during installation. This is only supported if there are no currently encrypted drives present on the system. Otherwise, decrypt before proceeding.

© SafeNet, Inc.

Chapter 12
Troubleshooting and Reporting Information

Switch from the Default to Legacy Pre-boot (Temporary)

In the unlikely event that you wish to temporarily change from the default pre-boot environment to the legacy pre-boot environment, perform the following steps to adjust the ProtectDrive settings:

1. While rebooting the system, press and hold the **[Shift]** key.
2. When the system boots in 16-bit mode, the 16-bit (legacy) ProtectDrive pre-boot logon screen displays.
3. Logon with your ProtectDrive credentials as usual.

Using this method to switch to 16-bit is only in effect until the system is rebooted again.

Switch from the Default to Legacy Pre-boot (Permanent)

If you wish to permanently change from the default pre-boot environment to the legacy pre-boot environment, contact SafeNet Technical Support for instructions.

Additionally, Technical Support maintains an extensive list of systems which SafeNet has validated that no pre-boot adjustment is necessary for use with ProtectDrive.

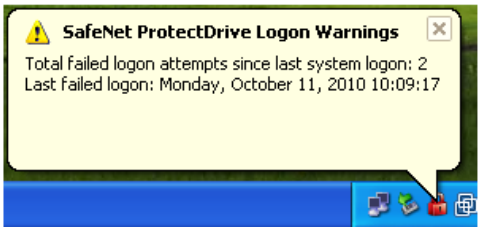
Disk Encryption Warning

If the **Display warning when disks are not fully encrypted** option (**PD Settings > Advanced > Encryption > Fixed Disks**) is set, and any of the drives are found to be unencrypted or partially encrypted, then the following ProtectDrive balloon tip will display right after the Windows Explorer shell loads:

SafeNet ProtectDrive Encryption Warning
All hard drives must be fully encrypted to ensure your system is secure.
The following drives have not been fully encrypted:
C:

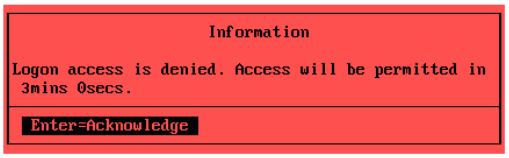
ProtectDrive User Authentication Activity Tracking

If the **Show Logon Information** and/or the **Show Unsuccessful Logon Warnings** options **(PD Settings > Advanced > User Interface)** are set, then after successful Windows authentication and right before the Windows Explorer shell loads, the following two ProtectDrive balloon tips will display. These messages alert the user of their ProtectDrive pre-boot authentication activity to-date:


SafeNet ProtectDrive Logon Warnings
Total failed logon attempts since last system logon: 2
Last failed logon: Monday, October 11, 2010 10:09:17

Incorrect Pre-boot Username and/or Password

Lockout policy defines the maximum number of failed pre-boot authentication attempts along with the lockout period. If a lockout occurs, ProtectDrive will display the screen shown below.



A countdown period will commence for a pre-determined period of time (this is defined in **PD Settings > Advanced > Lockout)**. The system will be inoperable during this time. In the above example, the user is denied access for three minutes.

Once access is regained, open the system's **Event Viewer** for details on failed logon attempts and other events. See page 184 for more on **Event Viewer**.

Pre-boot Log On Failure Due to System Inoperability

If any of the ProtectDrive system files and/or encrypted hard drive partitions experience corruption, the user may not be able to authenticate into the system at Pre-boot. In these isolated instances, an error screen will display an ACS Error Number, as shown in the example below. The user must communicate the error to the System Administrator.

Refer to *Appendix D* for a complete list of ACS Error Codes.

© SafeNet, Inc.

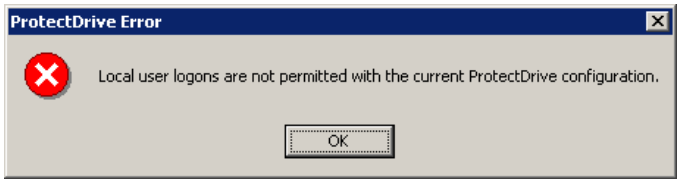
Disallowed Device Access Errors

The ProtectDrive Administrator can configure the system to disallow user access to specific devices, such as ports or removable media. If a user, whose device access control permissions are disabled, attempts to access a certain device, a message, similar to the following, will display.

If this occurs, the user should contact their System Administrator for further assistance.

Disallowed Local Windows Authentication Error

If the **Allow Local User Access** authentication System Policy option is disabled, and the user attempts to authenticate post-boot into the Local Windows by specifying *Local System Name* in the **Domain** field of the Windows Log On screen, then the following error will display:

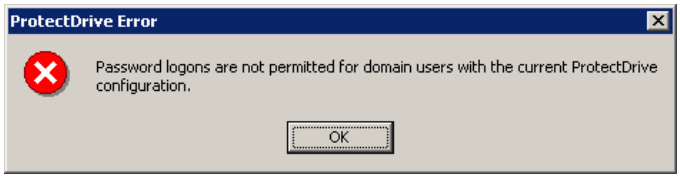


Note that if the **Allow Local Password Access** and **Allow Domain Password Access** options are both disabled, then pressing **CTRL-ALT-DEL** will have no effect.

Similarly, if the **Allow Domain Token Access** option is disabled, inserting a smart card/token will have no effect.

Disallowed Post-boot Windows Domain Authentication Error

If the user attempts to authenticate into the Windows Domain using the Windows Log On screen, but the **Allow Password Domain User Access** authentication System Policy option is disabled, then the following error will display:

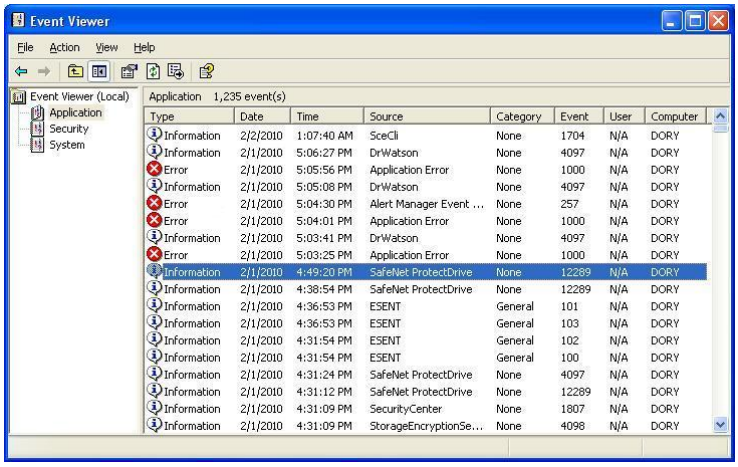

ProtectDrive Error
Password logons are not permitted for domain users with the current ProtectDrive configuration.
OK

Event Viewer Log

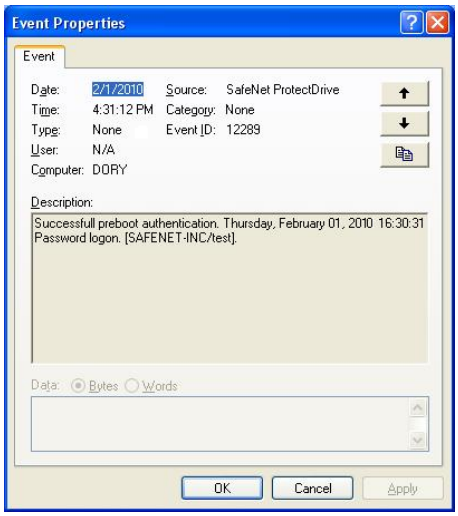
Careful monitoring of event logs can help you to identify and view details of ProtectDrive errors and events (such as successful or failed pre-boot authentication attempts), start and end times for drive encryption, and emergency recovery logins.

To access the **Event Viewer** from the Windows desktop:

1. Select **Start > Settings > Control Panel > Administrative Tools > Event Viewer**.
2. Click **Application** in the Event Viewer tree. Scroll through the list to view the events.


Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Application 1,235 event(s)
Type Date Time Source Category Event User Computer
Information 2/2/2010 1:07:40 AM SceCli None 1704 N/A DORY
Information 2/1/2010 5:06:27 PM DrWatson None 4097 N/A DORY
Error 2/1/2010 5:05:56 PM Application Error None 1000 N/A DORY
Information 2/1/2010 5:05:08 PM DrWatson None 4097 N/A DORY
Error 2/1/2010 5:04:30 PM Alert Manager Event ... None 257 N/A DORY
Error 2/1/2010 5:04:01 PM Application Error None 1000 N/A DORY
Information 2/1/2010 5:03:41 PM DrWatson None 4097 N/A DORY
Error 2/1/2010 5:03:25 PM Application Error None 1000 N/A DORY
Information 2/1/2010 4:49:20 PM SafeNet ProtectDrive None 12289 N/A DORY
Information 2/1/2010 4:38:54 PM SafeNet ProtectDrive None 12289 N/A DORY
Information 2/1/2010 4:36:53 PM ESENT General 101 N/A DORY
Information 2/1/2010 4:36:53 PM ESENT General 103 N/A DORY
Information 2/1/2010 4:31:54 PM ESENT General 102 N/A DORY
Information 2/1/2010 4:31:54 PM ESENT General 100 N/A DORY
Information 2/1/2010 4:31:24 PM SafeNet ProtectDrive None 4097 N/A DORY
Information 2/1/2010 4:31:12 PM SafeNet ProtectDrive None 12289 N/A DORY
Information 2/1/2010 4:31:09 PM SecurityCenter None 1807 N/A DORY
Information 2/1/2010 4:31:09 PM StorageEncryptionSe... None 4098 N/A DORY

3. Double-click on an event to display its properties and specific details.



© SafeNet, Inc.

Active Directory/ADAM Reporting Script

The **PDReport.vbs** reporting script is used to view the encryption status of all client computers in your Windows Domain. This tool is provided, in particular, for regulatory compliance audit purposes. The *\Tools* directory on the ProtectDrive distribution CD includes the **PDReport.vbs** script.

It is not necessary to modify the **PDReport.vbs** script before you run it, but you may choose to customize it.

Run this script on your Active Directory or ADAM server that is managing your ProtectDrive clients. The procedures to run this reporting script are slightly different on an Active Directory or ADAM server, and are described below.

When the reporting script is run, a **PDReport.csv** file is generated. This output includes a list of the client computer names and the following information, which can be easily viewed in a spreadsheet application, such as Microsoft® Office Excel:

- **PDStatus**—indicates **Active** if the client was accessible, and **Inactive** if the client was inaccessible.
- **LastUpdate**—displays the date and time the client was last updated by the ProtectDrive server.
- **EncryptedDrives**—displays the drives that are currently encrypted on the client. If this column is blank, the client has no encrypted drives.

ProtectDrive Server with Active Directory

You can run **PDReport.vbs** by double-clicking on the file name in the *\Tools* directory on the ProtectDrive distribution CD, or running it from the command line.

From the command line/DOS prompt, make sure you navigate to the *\Tools* directory where the script is located in order to run it.

ProtectDrive Server with ADAM

You must run **PDReport.vbs** from the command line/DOS prompt. Make sure you navigate to the *\Tools* directory where the script is located in order to run it, and use the following command format:

```
PDReport.vbs <server name where ADAM is installed>:<port number>
```

Example: `PDReport.vbs win2k3ent_server:50000`

Sample Report Output

ComputerName	PDStatus	LastUpdate(UTC)	EncryptedDrives
W2K3ENT-CLIENT1	Active	1/5/2011 18:10	C: D:
W2K3ENT-CLIENT2	Active	12/29/2010 06:08	C:
W2K3ENT-CLIENT3	Inactive		
W2K3ENT-CLIENT4	Active	1/2/2011 10:20	C:

© SafeNet, Inc.

Appendix A
Smart Card/Token & PIN User Authentication

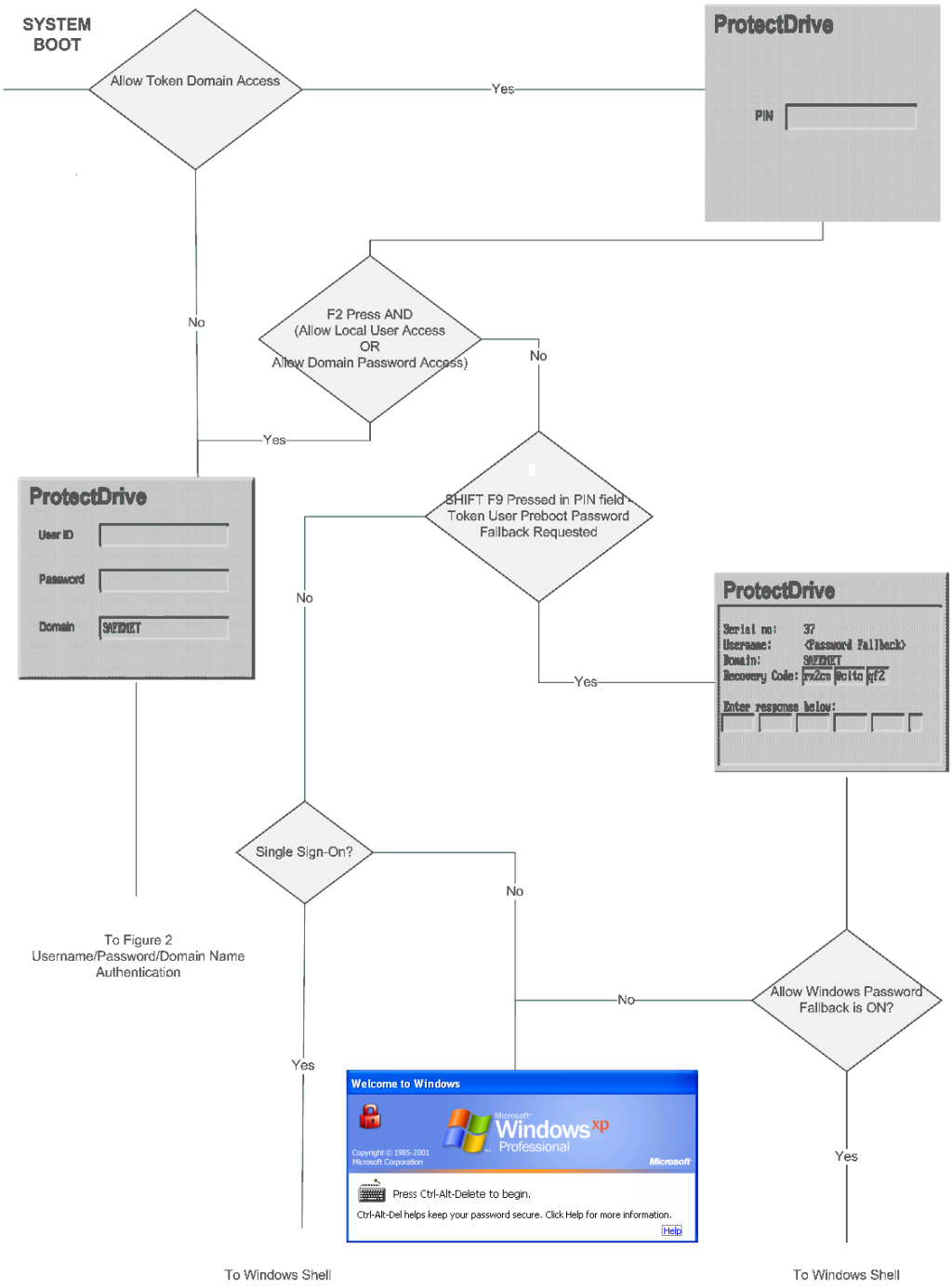


Figure 1
Smartcard/Token/PIN
Preboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Appendix B
Username/Password/Domain Authentication

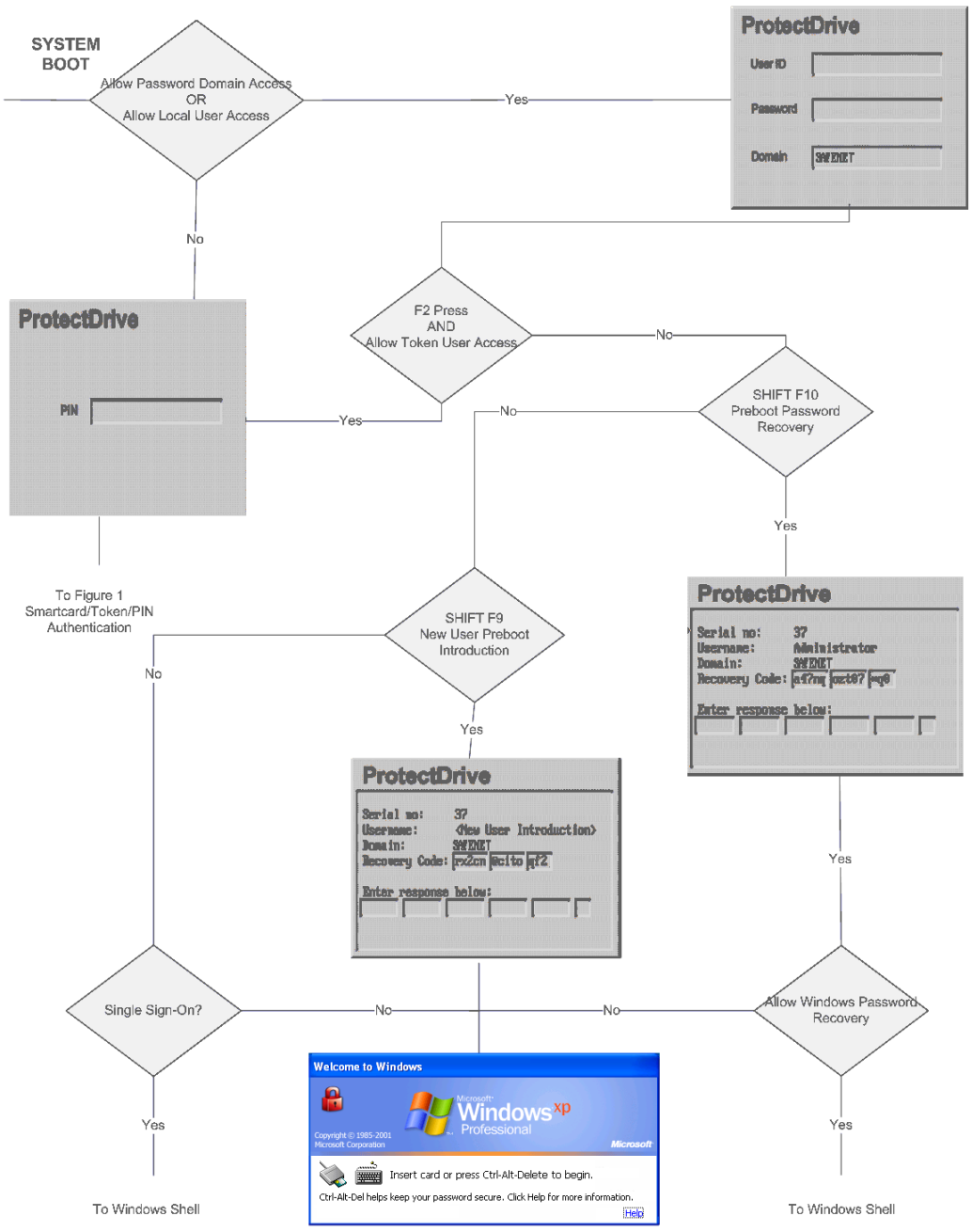


Figure 2
Username/Password/Domain Name
Preboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Appendix C
Post-boot User Authentication into Windows

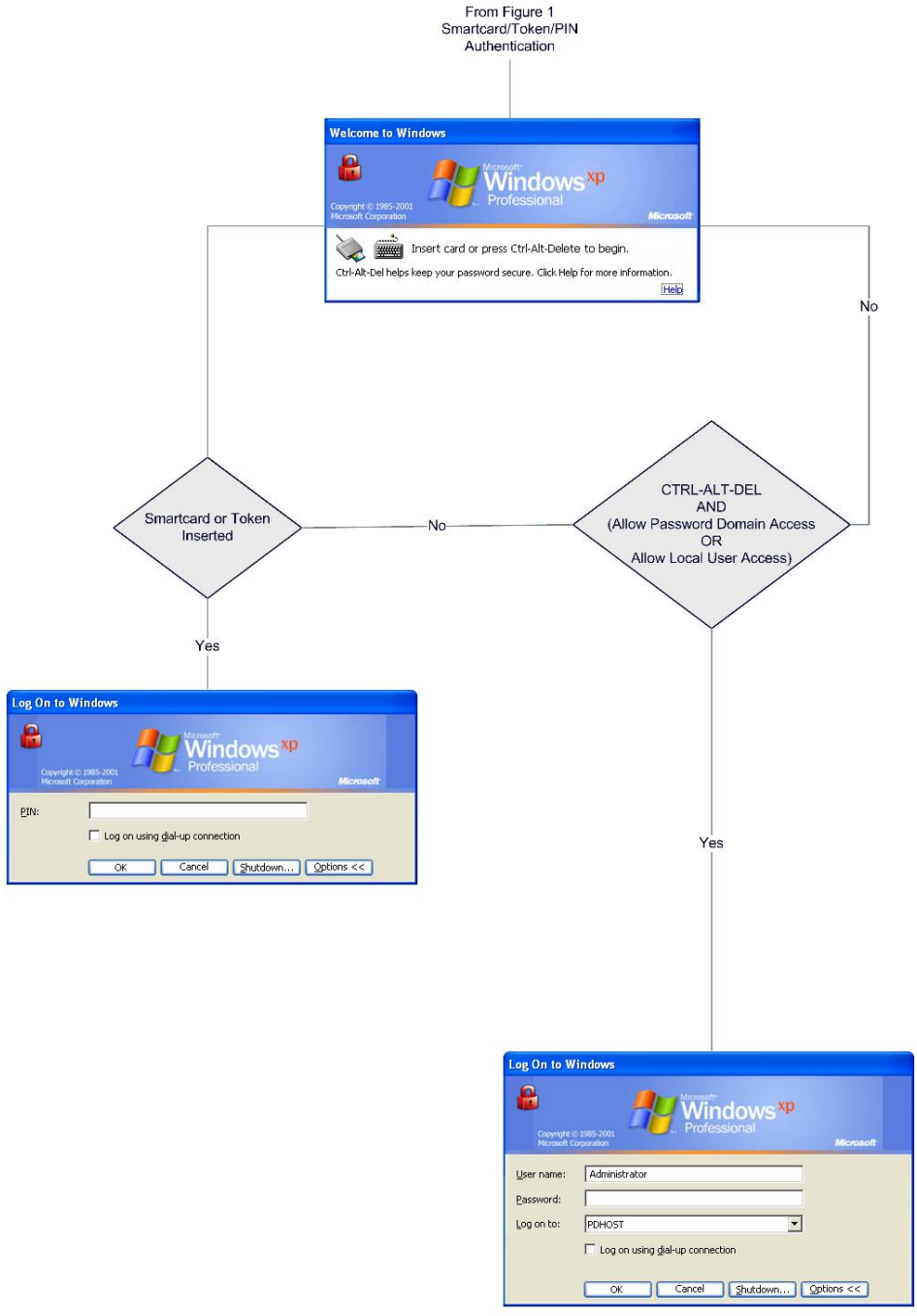


Figure 3
Smartcard/Token/PIN or
Username/Password/Domain
Postboot Authentication

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Appendix D
System Debug and ACS Error Messages

Before proceeding, familiarize yourself with the contents of Chapter 11 - RapidRecoveryTM Disaster Recovery Tools.

System Debug

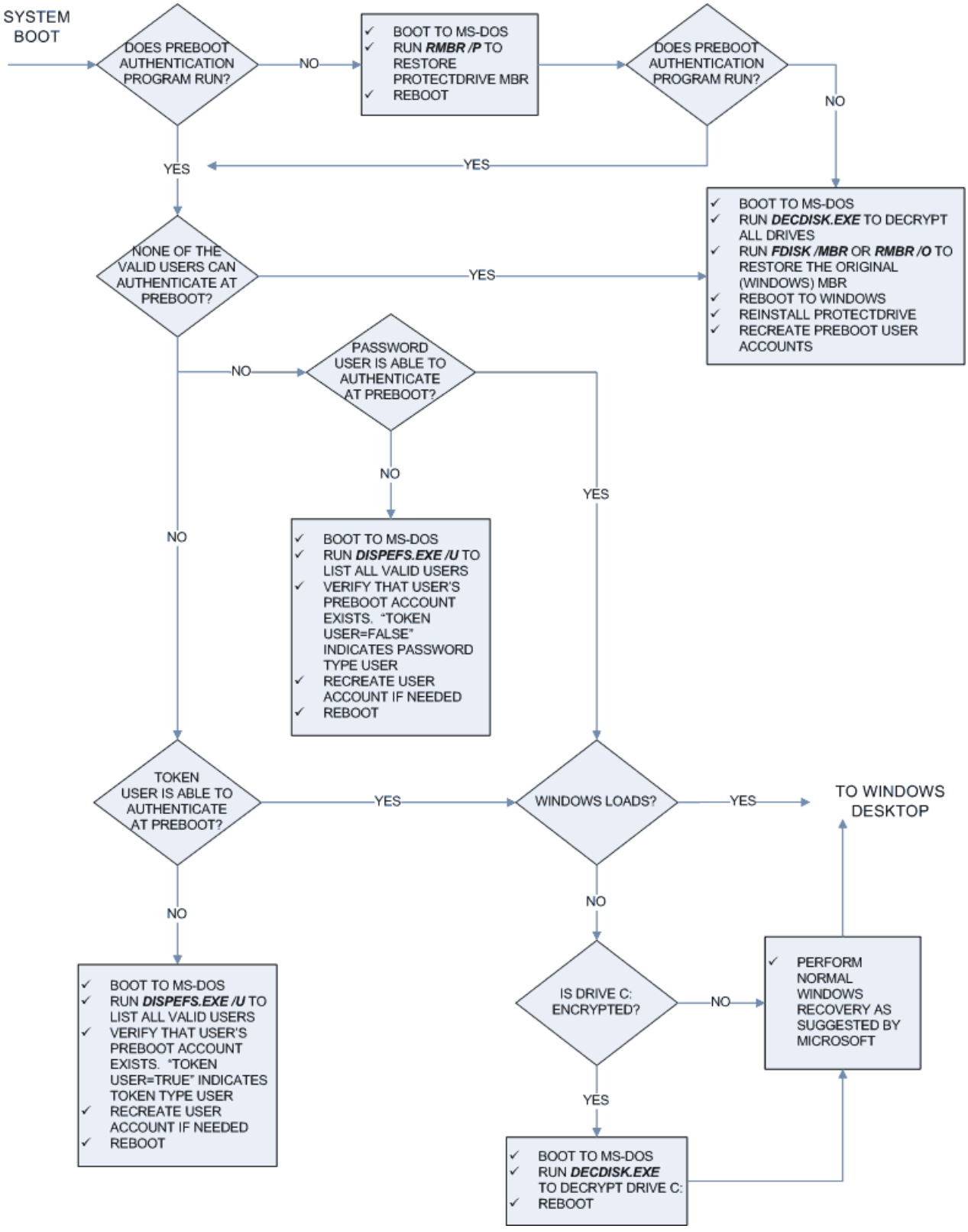
Problem	Fix
Password type account user can not be authenticated by the ProtectDrive Pre-boot Authentication program.	• Run *Dispefs.exe /u*. This will display a list of all users and their account types. Password type account users are indicated with **Token User = False** setting. If the user is shown to have a Password account type, then it is possible they are entering an invalid password. Passwords are case sensitive. Finally, if the user is positive they are entering the correct password, and no other user is able to log on, then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt.*

Smart Card/Token type account user can not be authenticated by the ProtectDrive Pre-boot Authentication program.	• Run *Dispefs.exe /u*. to list of all existing users and their account types. Smart Card/Token type account users are designated with **Token User = True** setting.
	
	Although a user may have one or more token accounts, it is possible that the Certificate contained by the token does not match the Certificate originally used for this user's record creation in the ProtectDrive Pre-boot User database. Note that users may have multiple records in the pre-boot user database. The **Hash** field displayed by *Dispefs.exe* /u is the same as the **Thumbprint** field displayed when certificate details are viewed in Windows.
	
	Finally, if the user is positive they are using a valid token, and no other user is able to log on, then the ProtectDrive files have become corrupt. See below for *ProtectDrive appears to be corrupt*.
	
	• Other alternatives include:
	
	  • If smart cards are used, try an alternative smart card reader.
	
	  • Remove and re-insert the smart card or token.
	
	  • Reboot the system, and then retry the smart card or token.

Problem	Fix
User successfully authenticates at Pre-boot but Windows does not boot.	• It's possible that one of the Windows system files is corrupt. If Drive **C** is not encrypted, proceed with normal Windows recovery. • If Drive **C** is encrypted, run **decdisk.exe** to decrypt the system drive and enable Windows Recovery tools access the system drive.
ProtectDrive Pre-boot Authentication Program does not run.	• If **rmbr /o** or another utility has replaced the ProtectDrive MBR, the Pre-boot Authentication program will not be run. • If the system drive is encrypted, the operating system will also fail to load. • If the system drive is not encrypted, but other drives are, the operating system will load but access to the encrypted drives will be prevented by the ProtectDrive driver. To recover from these situations, run **rmbr /p**.
ProtectDrive appears to be corrupt.	If ProtectDrive is corrupt, then one of the following is possible: • Pre-boot Authentication Program will not run or behaves strangely. • Valid users can not be authenticated at pre-boot. • Operating system fails to load. If none of the above sections apply or you failed to restore ProtectDrive to normal working order; then all the encrypted drives will need to be decrypted using **decdisk.exe**. If **decdisk.exe** is unable to access the ProtectDrive Embedded File System (EFS); then use the Recovery Files originally created by **backup.exe**. Once all the drives have been decrypted, run **rmbr /o** to restore the ProtectDrive MBR. It is possible to boot the operating system once the system drive has been decrypted. It is not possible to uninstall ProtectDrive until all drives are decrypted.

© SafeNet, Inc.

The following flowchart represents the system debug information listed above. It is included for additional information.



ACS Error Messages

The ProtectDrive Access Control System (ACS) becomes active when a computer with ProtectDrive installed boots up. If an error occurs during its initialization, the system will display an error message composed of an error number and a brief description.

Error numbers are composed of three components:

CTXX where:

C	is the module the error occurred in
T	identifies the type of error and
XX	is the actual error number

Module identifiers are:

0	Master Boot Loader (MBL)
1	VXBIOS
2	NetBSD
3	VROM

Type identifiers are:

0	Not used
1	Warning
2	Error
3	Fatal

The table starting on the next page lists all ACS errors, possible causes, and recommended recovery actions.

© SafeNet, Inc.

ACS Error	Component	Description	Possible Cause	Recovery Action
0301	MBL	Invalid master boot code checksum	MBR corruption MBR Trojan attack	Run rmbr.exe to recover the ProtectDrive MBR.
0305	MBL	Invalid VXBIOS -OR- Cannot boot from encrypted Removable Media (USB)	Signature, checksum or size verification of the VXBIOS failed possibly caused by disk corruption -OR- Removable Media does not have an OS	Contact SafeNet Support. -OR- Unplug Removable Media and reboot again. -OR- Modify the Boot Order in the BIOS configuration, and move the USB further down the device list.
0306	MBL	Invalid master boot record signature	MBR corruption MBR Trojan attack	Run rmbr.exe to recover the ProtectDrive MBR.
0307	MBL	No SafeNet partition info	Partition table corruption or change. Addition of fixed disk after ProtectDrive installation	Run rmbr.exe to recover the ProtectDrive MBR.
0313	MBL	Disk i/o error reading sector stack	Disk IO error (Hard disk failure) or partition table corruption	Run rmbr.exe to recover the ProtectDrive MBR.
0314	MBL	Disk i/o error reading VXBIOS	Disk IO error (Hard disk failure) or partition table corruption	Run rmbr.exe to recover the ProtectDrive MBR.
1100	VXBIOS	System Not Initialized	System could not load the disk encryption key or the DTE EFS is missing or corrupted.	Standard Recovery Procedure

ACS Error	Component	Description	Possible Cause	Recovery Action
1101	VXBIOS	EFS Protection incomplete due to extensive fragments	Fragmented disk	Standard Recovery Procedure, and then defrag the drive
1204	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size, or a read error occurred	Standard Recovery Procedure
1205	VXBIOS	VROM Status Error	VROM signature verification failed or the program loader reported an error.	Standard Recovery Procedure
1300	VXBIOS	Insufficient memory	Failed to allocate memory for the VROM Insufficient memory available	Try to free up resources.
1301	VXBIOS	GDA file load error	GDA file is missing or a read error occurred when tying to initialize encryption information	Standard Recovery Procedure
1310	VXBIOS	Cannot Init EFS	EFS corruption	Standard Recovery Procedure
1311	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred (Displayed after a ACS1204 error)	- - -
1312	VXBIOS	VXVECT save fail	Failed to store original disk interrupt service routine (ISR) address in the EFS super block EFS corruption	Standard Recovery Procedure
1313	VXBIOS	SBLK get fail	Failed to locate the EFS Super Block	Run rmbr.exe to attempt to restore the ProtectDrive MBR.
1314	VXBIOS	Info open fail	Missing VDX EFS file EFS corruption	Standard Recovery Procedure
1315	VXBIOS	Info write fail	EFS corruption	Standard Recovery Procedure

© SafeNet, Inc.

ACS Error	Component	Description	Possible Cause	Recovery Action
1316	VXBIOS	VROM EXEC fail	Failed to execute the VROM (Displayed after a ACS1205 error)	- - -
1317	VXBIOS	Info read fail	EFS corruption	Standard Recovery Procedure
1318	VXBIOS	Diskette boot fail	Master Boot Loader signature verification failed; Missing operating system on floppy disk	Use bootable floppy diskette; Eject floppy diskette from drive and boot from hard disk
1319	VXBIOS	GDA open fail	GDA file is missing when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1320	VXBIOS	GDA read fail	A read error occurred on the GDA file when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1321	VXBIOS	Boot fail	Master Boot Loader signature verification failed.	Standard Recovery Procedure
1322	VXBIOS	NetBSD Boot open fail	The required NetBSD Boot file is not in the EFS.	- - -
1323	VXBIOS	NetBSD Boot read fail	The required NetBSD Boot file is not in the EFS.	- - -
1324	VXBIOS	HMAC SHA-256 test fail	VxBIOS is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.

ACS Error	Component	Description	Possible Cause	Recovery Action
1325	VXBIOS	VxBIOS integrity check fail	VxBIOS is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
1326	VXBIOS	NB_Boot integrity check fail	NetBSD boot module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
1327	VXBIOS	CRYPdll integrity check fail	Pre-boot crypto module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
1328	VXBIOS	CRYPdll AES test fail	Pre-boot crypto module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.

© SafeNet, Inc.

ACS Error	Component	Description	Possible Cause	Recovery Action
1329	VXBIOS	NB_Kern integrity check fail	NetBSD main module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
2301	NetBSD	NetBSD AES test fail	NetBSD main module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
2302	NetBSD	NetBSD SHA-1 test fail	NetBSD main module is corrupted or has been tampered with.	Reboot. If the problem persists, perform Standard Recovery Procedure and install ProtectDrive from scratch. -AND- If the problem persists, contact SafeNet Support.
3301	VROM	Too many logon attempts	Forgotten password Corrupted user database	Log on as other user; Exercise user key recovery; Run dispefs.exe.
3302	VROM	I/O error reading disk	Corrupted EFS Hard disk failure	Standard Recovery Procedure
3304	VROM	An unknown error has occurred	Internal program error	Standard Recovery Procedure

ACS Error	Component	Description	Possible Cause	Recovery Action
3305	VROM	Configuration file has been corrupted	MAC check of configuration file failed Corrupted EFS	Standard Recovery Procedure
3306	VROM	User information has been corrupted	MAC check of user database entry failed Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows. User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3308	VROM	ProtectDrive Administrator information has been corrupted	MAC check of ProtectDrive Administrator failed; Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows. User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3309	VROM	Configuration file has been fatally corrupted	EFS corruption Hard disk failure	Standard Recovery Procedure
3310	VROM	Error occurred initializing the token	The token module could not be initialized and password logons are not allowed.	To diagnose this error further, contact SafeNet Support. To get access to the system, exercise the password fallback function.

© SafeNet, Inc.

Appendix E
Additional Guidance Regarding Security

Evaluated Versions of ProtectDrive

This chapter provides important guidance to users of evaluated versions of ProtectDrive. Evaluation of ProtectDrive is based on assumptions contained in a Security Target for the evaluation.

The Security Target describes the basis of the evaluation including:

- Threats that the security claims of ProtectDrive are designed to counter
- Environmental and organizational assumptions required to support the security claims
- Constraints to the configuration of the ProtectDrive required to support the security claims

When relying on an evaluated version of ProtectDrive, users should follow the recommendations in this appendix, refer to the evaluation Security Target, and refer to the Certification Report for guidance on use of the evaluated version of ProtectDrive.

The Security Target and the Certification Report can be found in the Common Criteria Evaluated Products List (EPL). This list, for ProtectDrive, may be found at:

http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

Both the Security Target and Evaluation Technical Report are available online on completion of an evaluation.

Guidance for Users of ProtectDrive

Further Reading Relevant to the CC Certification

The following documents should be read in conjunction with this manual:

- Security Target
- Certification Report
- Release Notes included on the distribution CD

Users are reminded that evaluated versions of ProtectDrive are based on assumptions contained in the evaluation Security Target. In particular, read the following chapters:

- Chapter 3 – Assumptions
- Chapter 4 – Security Objectives for the Environment

These chapters describe the responsibility of users and detail requirements needed to ensure that ProtectDrive product is used and administered securely.

Product Identification

To ensure that the copy of ProtectDrive you have is authentic and is the correct version:

Before Installation

- Check the product version number on the CD label. You should ensure that the label identifies the version as PD x.yy.zz, where x.yy.zz is the ProtectDrive version number. If you are using an evaluated version of ProtectDrive ensure that the version you are installing matches the version listed in the Evaluated Products List.
- If installing ProtectDrive from an electronic archive, then ensure that the file name is pd_x_yy_zz, where x_yy_zz is the version number.
- Ensure that the Customer Release Note (CRN) file on the distribution CD refers to the product version being used.

After Installation

Verify the version number of ProtectDrive after installation. Right-click on the ProtectDrive icon in the notification area, and then select **About SafeNet ProtectDrive**.

Verify that the version number displayed matches the expected version number of the installed software.

© SafeNet, Inc.

Organizational Requirements

Connections to Outside Systems

Those responsible for management of the systems in which ProtectDrive is used must ensure that no connections are provided to outside systems that would undermine the security features of ProtectDrive.

Guidance

Guidance should be provided that details the delivery, installation, configuration, administration and operation of ProtectDrive within an organization.

Tampering

The system on which the product is installed must have features that detect physical tampering and provide a clear indication to users that tampering has occurred. Users must be able to regularly check the system for indications of tampering.

Training

All users of ProtectDrive with Administrator privileges must receive sufficient training to enable them to securely administer ProtectDrive.

Users of ProtectDrive with administration privileges are responsible for implementing guidance that ensures ProtectDrive is installed, configured, administered, and operated in a secure manner consistent with the evaluated configuration.

Tokens

Smart cards or tokens used with ProtectDrive, for authentication, must provide an adequate level of security to protect authentication information and perform the functions required by ProtectDrive. This security may be gained though assurance of the smart card or token or a combination of smart card/token assurance combined with organizational procedures.

Users

Users of ProtectDrive must receive sufficient guidance and training to be able to fulfill their duties.

Device Permissions

ProtectDrive manages secure use of many device types. Control is based on system and user policy by independently setting read/write access permission for each device in the **PD Settings > Advanced > Default Permissions** group.

Guidance for the Operating System Configuration

General

ProtectDrive provides protection of information through pre-boot authentication and access control of peripheral devices combined with hard disk encryption. Once access is gained to a computer (by correct user authentication) the user is then responsible for ensuring that the computer is treated in accordance with organizational security policies for the level of information available.

Administrators of ProtectDrive are responsible for ensuring that the underlying operating system is correctly configured and complies with organizational security policies.

If the computer on which ProtectDrive is installed is a part of a network domain then the domain security policies must be correctly configured and comply with organizational security policies.

Password Policy

The operating system password policy must be configured in accordance with organizational policies and be consistent with ProtectDrive requirements. The following minimum settings should be used:

Enforce Password History	7 passwords
Maximum Password Age	In accordance with organizational policy
Minimum Password Age	1 day or greater if required by organizational policy
Minimum Password Length	6 characters or greater if required by organizational policy
Passwords Must Meet Complexity Requirements	Enabled
Store Password Using Reversible Encryption	Disabled

Screen Lock Feature

The operating system **Screen Lock** feature must be enabled and configured in accordance with organizational requirements. If the **Screen Lock** feature is not enabled and configured correctly, ProtectDrive security features may be subverted.

© SafeNet, Inc.

Information Relevant to Administrators of ProtectDrive

Operating Systems

Evaluated versions of ProtectDrive are tested on specific version of operating systems.

While the product will operate with a wider range of service packs and builds, if you wish to use it in its evaluated configuration, you should only use it on those specified in the most current ProtectDrive Customer Release Notes (CRN).

Evaluated Items

Note that the –Server Edition" of ProtectDrive has not been evaluated, and nor has the –Multiple Boot Manager" functionality. Furthermore, only the –Registered Product" has been evaluated.

Encryption Algorithm

To comply with Government advice, only the AES and Triple DES encryption algorithms have been evaluated and one these algorithms should be selected during installation. This will ensure that the correct components are installed and the choice of algorithms available for initial encryption will be limited to AES and Triple DES.

Display Warning When Disks Not Fully Encrypted

It is strongly recommended that this option be set ON in the evaluated configuration so that users are advised if the disk they are working on is not completely encrypted. If this is set to ON, the warnings will be displayed for all users.

Automatic Pre-boot Authentication

This option must be used with caution, and strictly as directed in the relevant chapter of this administration guide.

Show Unsuccessful Logon Warnings

This option should be set ON in the evaluated configuration so that the user is warned of unsuccessful logons.

Access Control

ProtectDrive offers a number of access control options: User ID and Password, Token and PIN, and emergency logon options.

Evaluated versions of ProtectDrive may not include all access control options. When using an evaluated version of ProtectDrive, users should refer to the evaluation Security Target to determine which options form part of the evaluated version. Only those access control options that form a part of the evaluated version of ProtectDrive should be enabled.

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Appendix F
iKey Management

iKey 1000

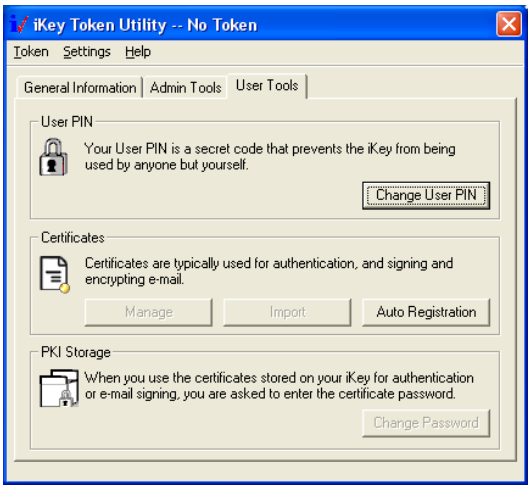
The SafeNet iKey 1000 tokens can easily be used in conjunction with ProtectDrive to provide secure two-factor authentication. This section briefly reviews how to manage iKey 1000s through the standard iKey SDK. Please refer to the *iKey 1000 Series Developer's Guide (SDK)* for more specific details.

The following procedure assumes that iKey 1000 software (including the device driver and iKeyAPI.DLL) are properly installed. For more specific details, refer to the documentation that accompanies the iKey 1000.

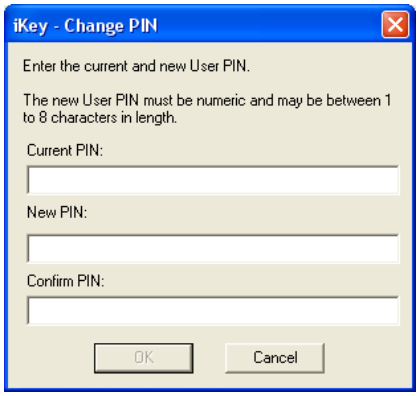
Manage the iKey 1000 Through the iKey SDK

To assign a user a PIN:

1. Insert the iKey 1000 token.
2. From the Windows desktop, select **Start > Programs > SafeNet > iKey Components > iKey Token Utility**.


iKey Token Utility -- No Token
Token
Settings
Help
General Information
Admin Tools
User Tools
User PIN
Your User PIN is a secret code that prevents the iKey from being used by anyone but yourself.
Change User PIN
Certificates
Certificates are typically used for authentication, and signing and encrypting e-mail.
Manage
Import
Auto Registration
PKI Storage
When you use the certificates stored on your iKey for authentication or e-mail signing, you are asked to enter the certificate password.
Change Password

3. Select the **User Tools** tab, and then click **Change User PIN.**


iKey - Change PIN
Enter the current and new User PIN.
The new User PIN must be numeric and may be between 1 to 8 characters in length.
Current PIN:
New PIN:
Confirm PIN:
OK
Cancel

4. Enter the current PIN (the factory default is **12345678**), enter and confirm the user's new PIN, and then click **OK**.

5. Click **OK** when prompted that the PIN change was successful.

6. Now you can add this user to the ProtectDrive database and register the iKey 1000 (shared key token) to the user. This can be performed from the **PD Users** tab, either locally in the ProtectDrive **Local Management Console** or centrally managed from the **ProtectDrive Management Console**.

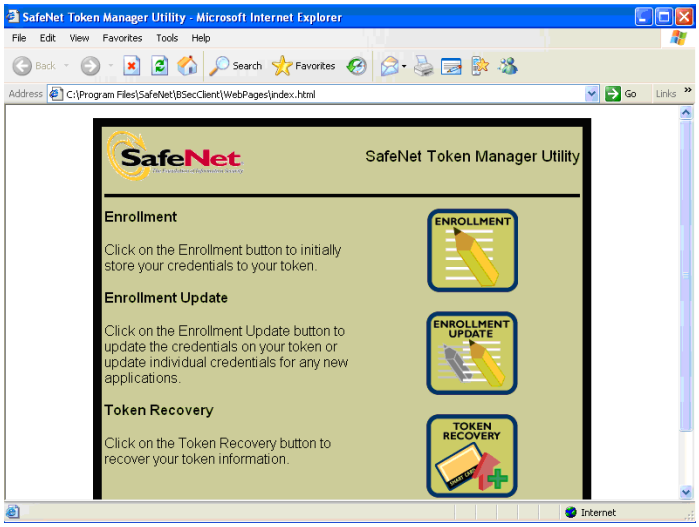
© SafeNet, Inc.

iKey 2032

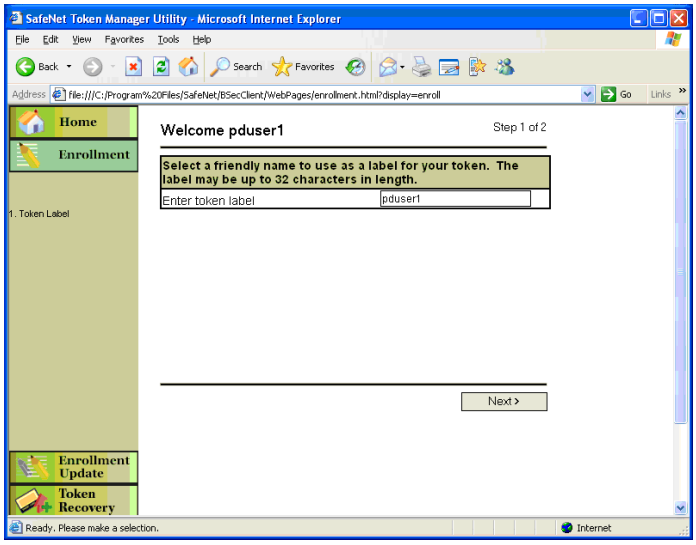
There are two ways to manage the iKey 2032—through the SafeNet Token Manager Utility, or through Web Enrollment.

SafeNet Token Manager Utility

1. Insert the iKey 2032 token. (The light on the token should remain lit.)
2. From the Windows desktop, select **Start > Programs > SafeNet > SafeNet Token Manager Utility**.

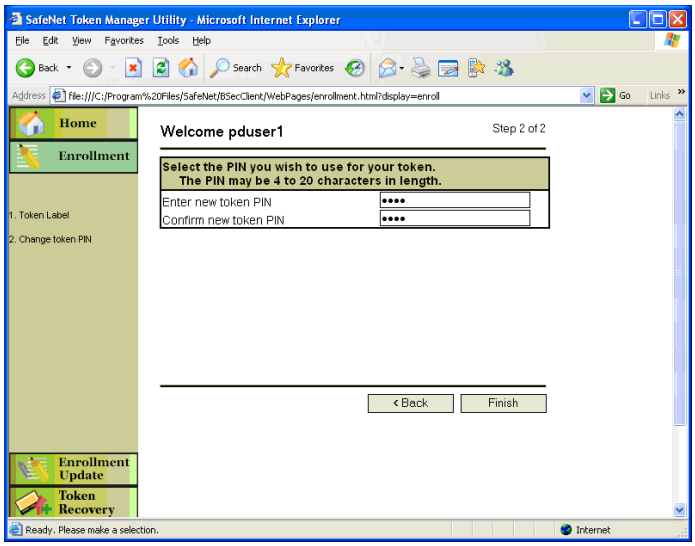

SafeNet Token Manager Utility - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address C:\Program Files\SafeNet\BSecClient\WebPages\index.html
SafeNet
SafeNet Token Manager Utility
Enrollment
Click on the Enrollment button to initially store your credentials to your token.
ENROLLMENT
Enrollment Update
Click on the Enrollment Update button to update the credentials on your token or update individual credentials for any new applications.
ENROLLMENT UPDATE
Token Recovery
Click on the Token Recovery button to recover your token information.
TOKEN RECOVERY
Internet

3. Click **Enrollment**.
4. When prompted, enter a label for this token (up to 32 characters). This can be the user's name, or anything else you choose.

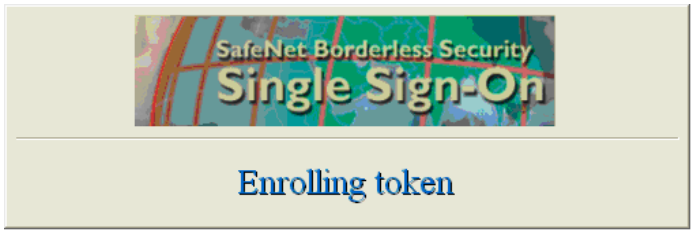

SafeNet Token Manager Utility - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address file:///C:/Program%20Files/SafeNet/BSecClient/WebPages/enrollment.html?display=enroll
Home
Enrollment
1. Token Label
Welcome pduser1
Step 1 of 2
Select a friendly name to use as a label for your token. The label may be up to 32 characters in length.
Enter token label
pduser1
Next >
Enrollment Update
Token Recovery
Ready. Please make a selection.
Internet

5. Click **Next**.

6. When prompted, enter and confirm a PIN for this token (4 to 32 alphanumeric characters).



7. Click **Finish**. The following pop-up window displays. Enrollment may take a few moments to complete. You may also see the message, *Communicating with server*.



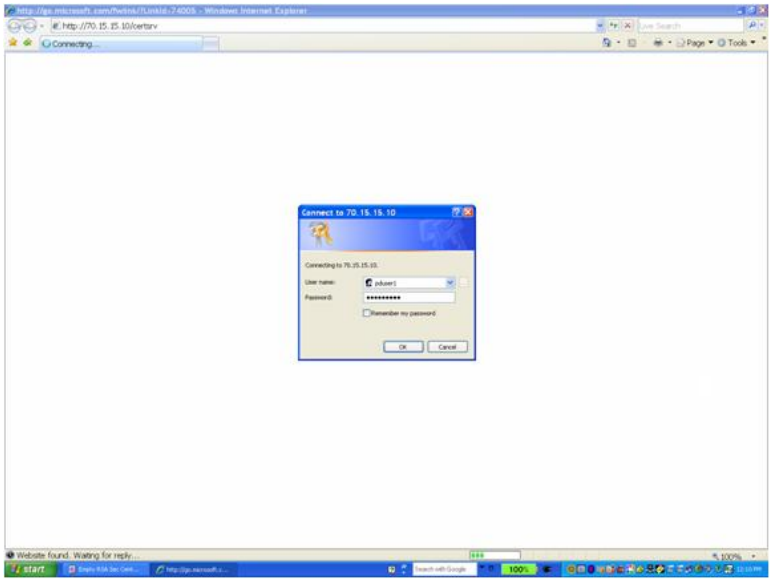
8. Click **OK** when enrollment is complete.

© SafeNet, Inc.

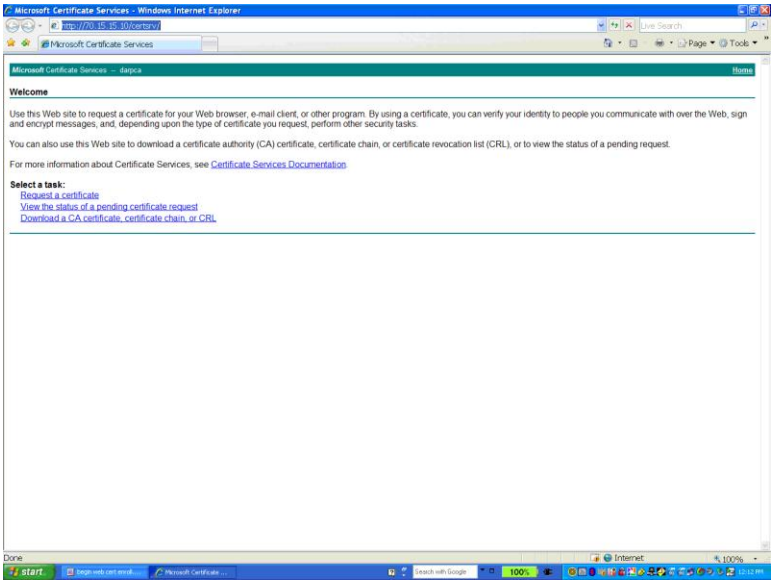
Web Enrollment

1. Request a certificate. Open Windows Internet Explorer and type in the URL of your CA using the following format: *http://<IP address of CA>/certsrv*. For example: http://70.15.15.10/certsrv

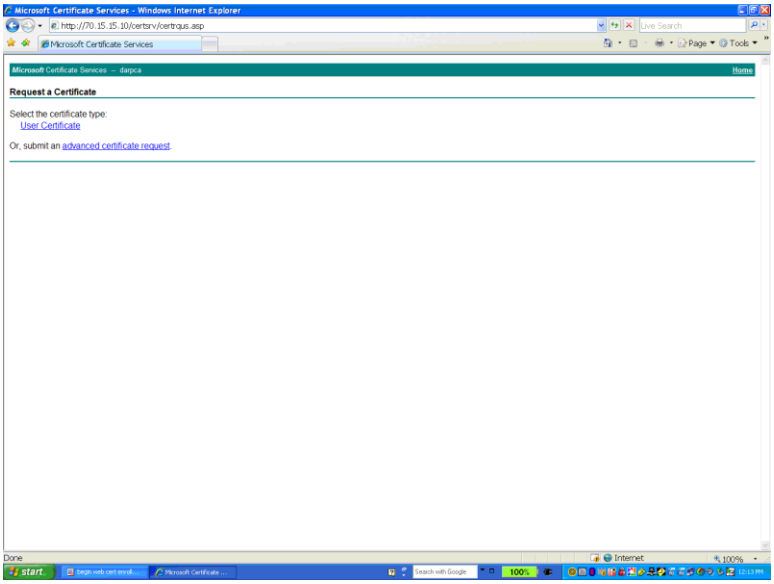
2. If prompted, enter a valid user name and password. Supply the credentials of the user requesting the certificate, and then click **OK**.



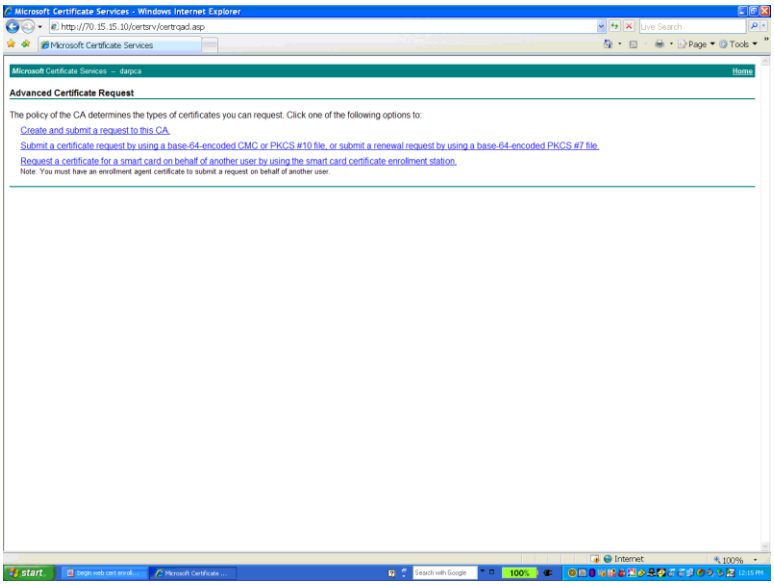
3. Once connected, a **Welcome** screen displays for **Microsoft Certificate Services** for your CA.


Microsoft Certificate Services - Windows Internet Explorer
Microsoft Certificate Services
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

4. Click **Request a certificate**. The following screen displays:

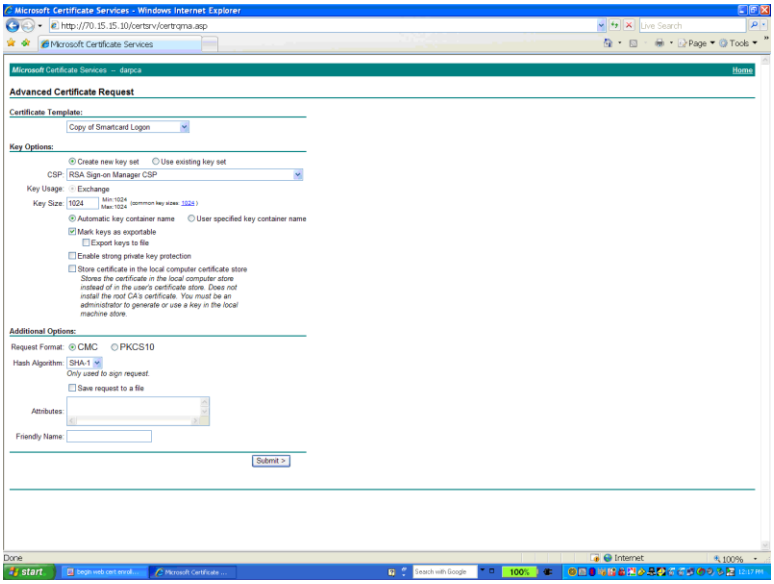


5. Click **advanced certificate request**. The following screen displays:


Microsoft Certificate Services - Windows Internet Explorer
http://70.15.15.10/certsrv/certrqad.asp
Microsoft Certificate Services
Microsoft Certificate Services -- darpca
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.
Internet
100%

© SafeNet, Inc.

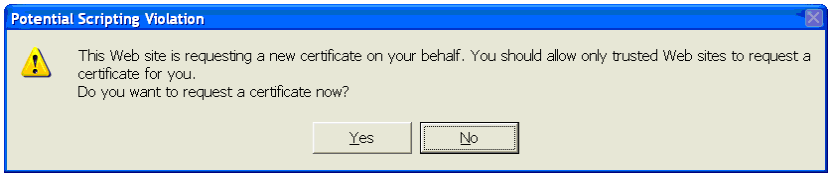
6. Click **Create and submit a request to this CA**. The following screen displays:



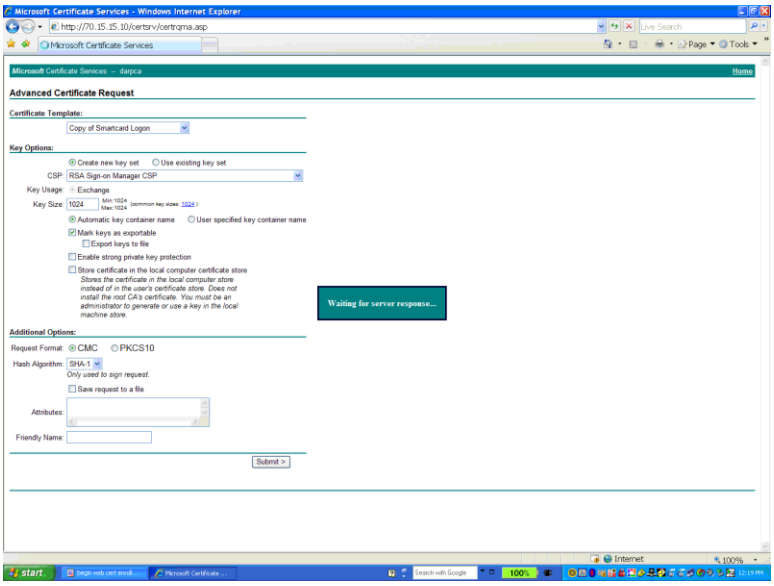
7. Select the following options as described below. For all other options, retain the default settings.

   - **Certificate Template**—Select **Copy of Smartcard Logon**.
   - **CSP**—Select **RSA Sign-on Manager CSP**.
   - **Mark keys as exportable**—Select this check box.

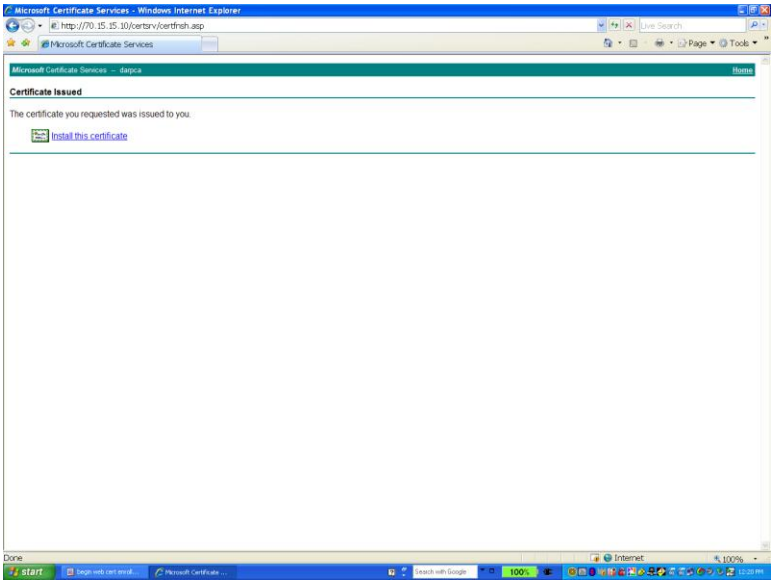
8. Click **Submit** to continue. The following message displays:


Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?
Yes
No

9. Click **Yes** to continue. You may note the message, *Waiting for server response...* This may take a few moments.

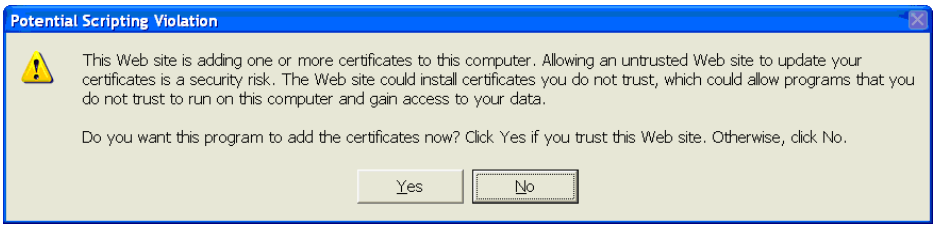

Microsoft Certificate Services - Windows Internet Explorer
Advanced Certificate Request
Waiting for server response...

10. When the **Certificate Issued** screen displays, click **Install this certificate**.

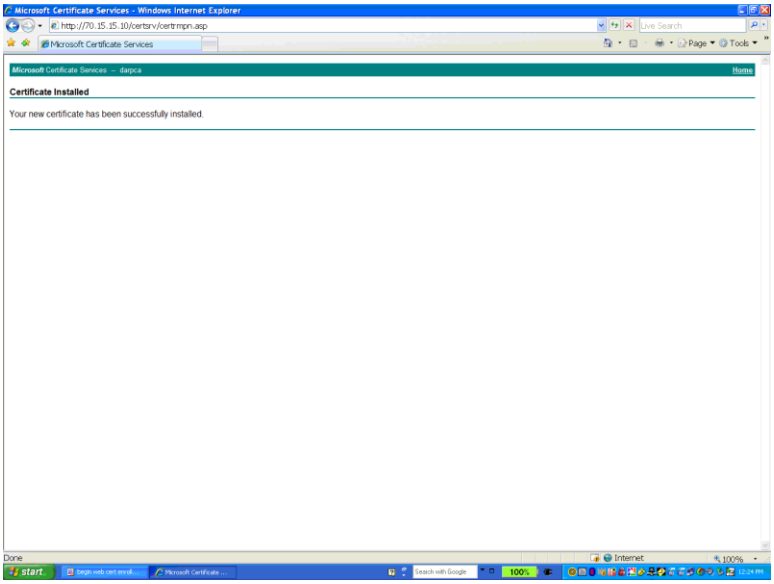

Microsoft Certificate Services - Windows Internet Explorer
Certificate Issued
The certificate you requested was issued to you.
Install this certificate

© SafeNet, Inc.

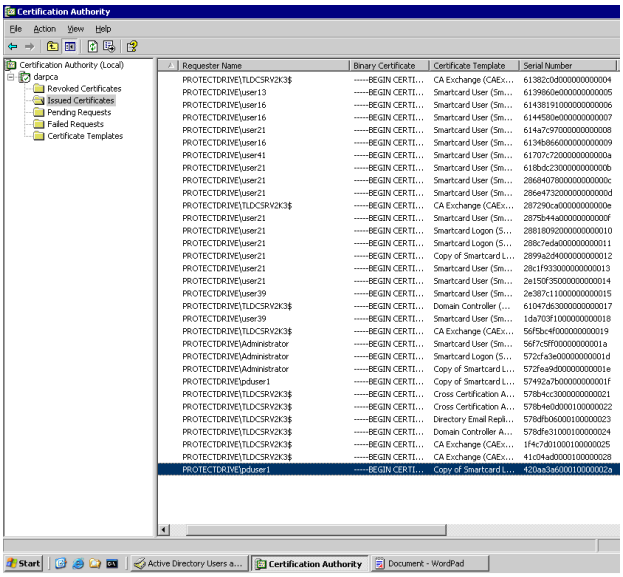
11. If you are prompted to do so, enter the PIN of the SD800 token. You may also receive the following warning:


Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

12. Click **Yes** to continue. The following screen displays:


Microsoft Certificate Services - Windows Internet Explorer
Certificate Installed
Your new certificate has been successfully installed.

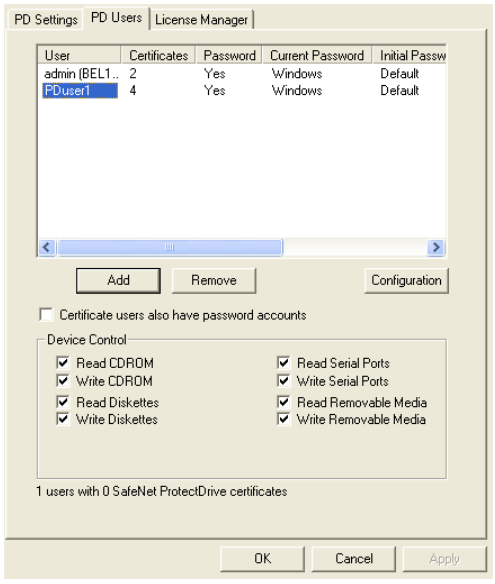
13. Your certificate should now be on your token and in the local machine store. Note the serial number for this certificate. It can be compared to the list of issued certificates on the CA (refer to the example below).



14. Log off this user and log back into the Windows domain by reinserting the token at the Windows logon prompt.

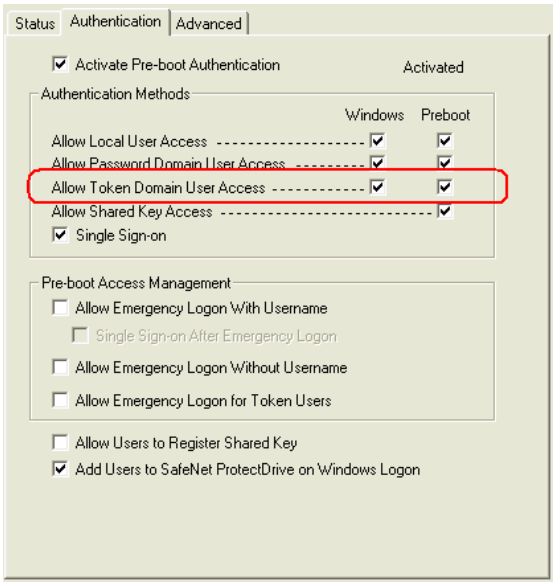
15. Enter the PIN at the prompt. Login should be successful with the certificate. Logging in this way will ensure the user is updated as a certificate user in the ProtectDrive users database.

16. Open the ProtectDrive **Local Management Console**, and note that the user name and certificate entry displays on the **PD Users** tab.



© SafeNet, Inc.

17. Select **PD Settings > Authentication**. Verify the **Allow Token Domain User Access** check box is selected for **Windows** and **Preboot** for this machine in Active Directory (for remotely managed machines), or in the **Local Management Console** (for locally managed machines).



18. Restart the machine.

19. Enter the PIN at the ProtectDrive pre-boot authentication (PBA) prompt. Four messages should follow:

    - *Initializing token*
    - *Searching for token certificate*
    - *Deciphering user key*
    - *Deciphering disk key*

20. After passing PBA, the certificate is handed off to Windows, and domain login proceeds automatically with Single Sign-on enabled.

THIS PAGE INTENTIONALLY LEFT BLANK

© SafeNet, Inc.

Appendix G
Supported Smart Cards, Tokens, and Readers

This appendix summarizes the smart cards, tokens, and smart card readers supported by the current version of ProtectDrive, which provide two-factor authentication prior to operating system startup.

This information is constantly evolving. If you do not see a specific smart card, token, or reader on this list, please contact Technical Support, as there may be more information available.

Smart Cards

Smart Card	Last Version Tested
ActivCard Client/Gold	9.4.0 - 32bit
Aladdin Card OS eToken 32k	9.4.0 - 32bit
Aladdin Card OS eToken 64k	9.4.0 - 32bit
Aladdin Java eToken 72k	9.4.0 - 32bit
Axalto Cyberflex 64k V1 (Schlumberger)	9.4.0 - 32bit
Axalto Cyberflex 64k V2c	9.4.0 - 32bit
Nexus Smartcard	9.4.0 - 32bit
SafeNet 330 (non-FIPS)	9.4.0 - 32bit
SafeNet 330 (FIPS)	8.4.0 - 16 bit; 9.4.0 - 32bit
SafeNet 330 U	9.4.0 - 32bit
SafeNet 330 I	9.4.0 - 32bit
SafeNet 330 GSA1	9.4.0 - 32bit
SafeNet 330 GSA2	9.4.0 - 32bit
SafeNet 330 GSA3	8.4.0 - 16 bit; 9.4.0 - 32bit
SafeNet 330 M	9.4.0 - 32bit
SafeNet 400	8.4.0 - 16 bit; 9.4.0 - 32bit
Siemens CardOS 4.3B	8.4.0 - 16 bit; 9.4.0 - 32bit
RSA SecurID 5100	9.4.0 - 32bit
Gemalto .NET	9.4.0 - 32bit
CAC - Axalto Access 64K	9.4.0 - 32bit
CAC - Gemalto Access 64KV2	9.4.0 - 32bit
CAC - Gemalto GCX4 72K DI	9.4.0 - 32bit
CAC - Gemalto TOPDLGX4 144	9.4.0 - 32bit
CAC - GemPlus GXP3 64V2N	9.4.0 - 32bit
CAC - Oberthur CosmopolIC V4	9.4.0 - 32bit
CAC - Oberthur ID One V5.2 Dual	9.4.0 - 32bit
CAC - Oberther ID One V5.2a Dual	9.4.0 - 32bit
CAC - Schlumberger Access 32K V2	9.4.0 - 32bit

Tokens

Token	Last Version Tested
Aladdin eToken PRO 16k	9.4.0 - 32bit
Aladdin eToken PRO 32k	8.4.0 - 16 bit; 9.4.0 - 32bit
Aladdin eToken PRO 32k (4.2b) FIPS	9.4.0 - 32bit
Aladdin eToken PRO 64k	9.4.0 - 32bit
Aladdin eToken PRO 64k (4.2b) FIPS	9.4.0 - 32bit
Aladdin eToken NG-OTP 32k	9.4.0 - 32bit
Aladdin eToken PRO Anywhere (Java)	9.4.0 - 32bit
Aladdin eToken PRO 72k (Java)	9.4.0 - 32bit
Aladdin eToken PRO 72k (Java) FIPS	9.4.0 - 32bit
Aladdin eToken NG-OTP 72k (Java)	9.4.0 - 32bit
Aladdin eToken NG-FLASH 72k (Java)	9.4.0 - 32bit
Aladdin eToken PRO 64k (4.2b)	9.4.0 - 32bit
SafeNet Borderless Security iKey™ 1000	8.4.0 - 16 bit; 9.4.0 - 32bit
SafeNet Borderless Security iKey™ 2032	8.4.0 - 16 bit; 9.4.0 - 32bit
SafeNet Borderless Security iKey™ 4000	9.4.0 - 32bit
KOBIL mIDentity XL (Siemens SIM)	9.4.0 - 32bit
RSA SecurID 800 Rev A	8.4.0 - 16 bit; 9.4.0 - 32bit
RSA SecurID 800 Rev D	8.4.0 - 16 bit; 9.4.0 - 32bit

© SafeNet, Inc.

Smart Card Readers

Smart Card Reader	Last Version Tested
Dell420 Built In	9.4.0 - 32bit
Dell D600 Built In (O2Micro OZ711EC1)	9.3.0 - 32bit
Dell D610 Built In (TI PCI 6515)	9.3.0 - 32bit
Dell D620 Built In (O2Micro OZ711E0 CCID SC)	9.4.0 - 32bit
Dell D630 Built In (USB - CCID)	9.4.0 - 32bit
Dell D810 Built In (TI PCI 6515)	9.4.0 - 32bit
Dell D820 Built In (O2Micro OZ711E0 CCID SC)	9.0.0 - 32bit
Dell D830 Built In (USB - CCID)	9.4.0 - 32bit
Dell E4300 Built In	9.4.0 - 32bit
Dell E6400 Built In	9.4.0 - 32bit
Fujitsu 9210 Built In	9.4.0 - 32bit
HP 6930 Built In	9.4.0 - 32bit
HP 8530 Built In	9.4.0 - 32bit
Gemplus GPR400 PCMCIA (DKR 600)	9.3.0 - 32bit
Gemplus GemPC Card PCMCIA (DKR 601)	9.4.0 - 32bit
Omnikey CardMan Mobile PCMCIA 4040 (DKR 701)	9.4.0 - 32bit
SCM SCR 241 PCMCIA Smart Card Reader (DKR 800)	9.4.0 - 32bit
SCM SCR243 PCMCIA Smart Card Reader	9.4.0 - 32bit
Gemplus GemPC 430 USB (DKR 630)	9.4.0 - 32bit
Gemplus GemPC USB Smart Card Reader (DKR 631)	9.4.0 - 32bit
Omnikey 3121 USB Smart Card Reader (DKR 731)	9.4.0 - 32bit
SCM SCR 331 USB Smart Card Reader (DKR 830)	9.4.0 - 32bit
Gemplus GemPC Twin (CCID)	9.4.0 - 32bit
Precise 200 MC	9.4.0 - 32bit
Precise 250 MC	9.4.0 - 32bit
Reflex V2 USB (Schlumberger)	9.4.0 - 32bit
Dell Smartcard Keyboard	9.4.0 - 32bit
Precise 100 SmartCard Keyboard	9.1.0 - 32bit
SCM SCR335 USB Smart Card Reader	9.4.0 - 32bit
SCM SCR3310/v2.0 USB Smart Card Reader	9.4.0 - 32bit
SCM SCR3500 USB Smart Card Reader (SCR 355)	9.4.0 - 32bit
SCM SDI010 USB Smart Card Reader	9.4.0 - 32bit
SCM SCR3340 ExpressCard54 Smart Card Reader	9.4.0 - 32bit

Removable Devices

Efforts have been made to ensure ProtectDrive is compatible with all removable media. However, some third-party removable media security software will interfere with ProtectDrive, and in most of these cases, is not recommended.

Most version 1.0 and 2.0 USB removable devices and USB hard drives should work with ProtectDrive.

END OF DOCUMENT

© SafeNet, Inc.